(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08316951 A**

(43) Date of publication of application: **29 . 11 . 96**

(51) Int. Cl **H04L 9/06**
H04L 9/14
H04Q 7/38
H04B 14/04
// G09C 1/00

(21) Application number: **07123369**

(22) Date of filing: **23 . 05 . 95**

(71) Applicant: **HITACHI LTD**

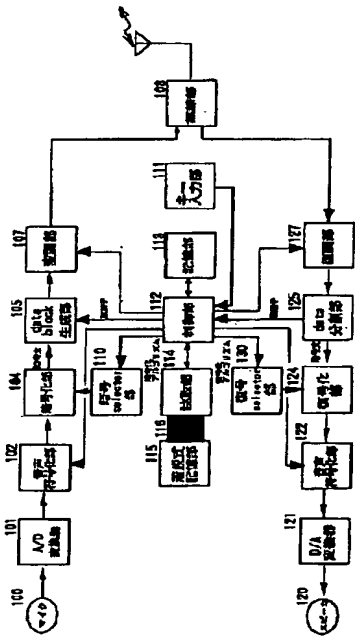
(72) Inventor: **KOIDE AYUMI**
KUROKI YOSHINORI

(54) RADIO COMMUNICATION TERMINAL, RADIO BASE STATION, AND COMMUNICATION SYSTEM PROVIDED WITH THEM

(57) Abstract:

PURPOSE: To provide an attachable/detachable storage device and a radio communication terminal which flexibly and easily copes with new ciphering or the like by the attachable/detachable storage device where ciphering algorithms are stored.

CONSTITUTION: An attachable/detachable storage part 115 where plural ciphering algorithms, identifiers corresponding to these ciphering algorithms in 1:1, and a ciphering table showing the correspondence relations between these identifiers and ciphering algorithms are stored is set to a setting part 116 where it can be set without opening the main body cover. An ciphering algorithm is selected by a cipher selection part 110, and voice data is ciphered in a ciphering part 104 based on the arbitrary selected ciphering algorithm to output a cipher text. A cipher data block generation part 105 refers to the ciphering table to read out the identifier corresponding to the selected ciphering algorithm and adds it to the cipher to output a cipher data block.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－316951

(43)公開日　平成８年(1996)11月29日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06			Ｈ０４Ｌ	9/02	Ｚ
	9/14			Ｈ０４Ｂ	14/04	Ｄ
Ｈ０４Ｑ	7/38		7259－5Ｊ	Ｇ０９Ｃ	1/00	
Ｈ０４Ｂ	14/04			Ｈ０４Ｂ	7/26	１０９Ｒ
// Ｇ０９Ｃ	1/00			Ｈ０４Ｑ	7/04	Ｄ

審査請求　未請求　請求項の数35　ＯＬ　（全 38 頁）

(21)出願番号　特願平7－123369

(22)出願日　平成７年(1995)５月23日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　小出　歩
神奈川県横浜市戸塚区戸塚町216番地株式会社日立製作所情報通信事業部内

(72)発明者　黒木　芳徳
神奈川県横浜市戸塚区戸塚町216番地株式会社日立製作所情報通信事業部内

(74)代理人　弁理士　小川　勝男

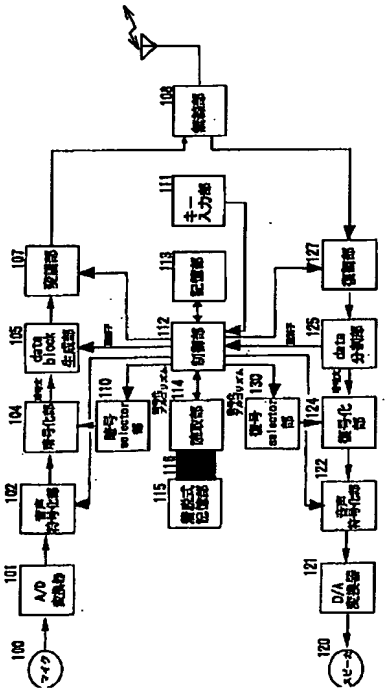
(54)【発明の名称】　無線通信端末、無線基地局及びこれらを有する通信システム

(57)【要約】

【目的】本発明は、暗号化アルゴリズムを記憶した着脱記憶装置により柔軟、かつ容易に新しい暗号化等へ対応できる無線通信端末及び着脱式記憶装置提供するものである。

【構成】複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する着脱式記憶部１１５を、本体カバーを開けずに装着可能とした装着部１１６へ装着し、暗号選択部１１０で暗号化アルゴリズムを選択し、暗号化部１０４でこの選択された任意の暗号化アルゴリズムに基づいて音声データを暗号化し暗号文を出力する。また、暗号データブロック生成部１０５で選択された暗号化アルゴリズムに対応する識別子を暗号化テーブルを参照して読みだし前記暗号文に付加して暗号データブロックを出力する。

図 1



1

【特許請求の範囲】

【請求項１】入力された音声をディジタル化し暗号化し通信を行う無線通信端末において、

装着部と、

前記装着部に着脱可能に装着され、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、

前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、

前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が出力する前記音声符号化データを暗号化し暗号文を出力する暗号化部と、

前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、

前記暗号データブロック生成部が出力する前記暗号データブロックに変調を施し変調データを出力する変調処理部と、

前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線通信端末。

【請求項２】基地局と多元接続により通信を行う無線通信端末において、

前記基地局が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、

前記無線受信部が取り出す変調信号に復調処理を施し誤り訂正符号化データブロックを取り出し出力する誤り復調処理部と、

前記復調処理部が出力する前記誤り訂正符号化データブロック中の誤りを検出し誤りを訂正し暗号データブロックを出力する誤り訂正符号化部と、

前記誤り訂正符号化部が出力する前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ出力するデータ分割部と、

複数の該復号化アルゴリズムと該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する着脱可能な記憶部と、

前記記憶部を装着する装着部と、

前記記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と、

前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部と、

前記復号化に接続され前記音声符号化データを復号しディジタル音声を出力する音声復号化部と、

2

前記音声復号化部の出力する前記ディジタル音声をアナログ化しアナログ音声を出力するアナログ変換部と、

前記アナログ変換部の出力するアナログ音声を外部に出力する音声出力部と、を有する無線通信端末。

【請求項３】アナログ音声が入力される音声入力部と、

前記音声入力部から入力される前記アナログ音声をディジタル音声信号に変換し出力するディジタル変換部と、

前記ディジタル変換部が出力する前記ディジタル音声信号を音声符号化データに音声符号化し出力する音声符号化部と、

複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、

前記複数の暗号化アルゴリズムのうちの何れか一つを選択する暗号選択部と、

前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が出力する前記音声符号化データを暗号化し暗号文を出力する暗号化部と、

前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、

前記暗号データブロック生成部が出力する前記暗号データブロックに誤り訂正符号化を施し誤り訂正符号化データブロックを出力する誤り訂正符号化部と、

前記誤り訂正符号化部が出力する前記誤り訂正符号化データブロックに変調を施し変調データを出力する変調処理部と、

前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線通信端末。

【請求項４】基地局と多元接続により通信を行う無線通信端末において、

前記基地局が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、

前記無線受信部が取り出す変調信号に復調処理を施し誤り訂正符号化データブロックを取り出し出力する誤り復調処理部と、

前記復調処理部が出力する前記誤り訂正符号化データブロック中の誤りを検出し誤りを訂正し暗号データブロックを出力する誤り訂正符号化部と、

前記誤り訂正符号化部が出力する前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ出力するデータ分割部と、

複数の該復号化アルゴリズムと、該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、

前記記憶部に記憶される前記復号化テーブルを参照し前

記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と、
前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部と、
前記復号化に接続され前記音声符号化データを復号しディジタル音声を出力する音声復号化部と、
前記音声復号化部の出力する前記ディジタル音声をアナログ化しアナログ音声を出力するアナログ変換部と、
前記アナログ変換部の出力するアナログ音声を外部に出力する音声出力部と、を有する無線通信端末。

【請求項５】アナログ音声が入力される音声入力部と、
前記音声入力部から入力される前記アナログ音声をディジタル音声信号に変換し出力するディジタル変換部と、
前記ディジタル変換部が出力する前記ディジタル音声信号を音声符号化データに音声符号化し出力する音声符号化部と、
外部ディジタルデータを入力するための外部インタフェース部と、
前記音声符号化データと前記外部ディジタルデータとのいずれか一方を選択し出力するデータ選択部と、
複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、
前記複数の暗号化アルゴリズムのうちの何れか一つを選択する暗号選択部と、
前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記データ選択部により選択されるデータを暗号化し暗号文を出力する暗号化部と、
前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、
前記暗号データブロック生成部が出力する前記暗号データブロックに誤り訂正符号化を施し誤り訂正符号化データブロックを出力する誤り訂正符号化部と、
前記誤り訂正符号化部が出力する前記誤り訂正符号化データブロックに変調を施し変調データを出力する変調処理部と、
前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線通信端末。

【請求項６】基地局と多元接続により通信を行う無線通信端末において、
前記基地局が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、
前記無線受信部が取り出す変調信号に復調処理を施し誤り訂正符号化データブロックを取り出し出力する誤り復調処理部と、

前記復調処理部が出力する前記誤り訂正符号化データブロック中の誤りを検出し誤りを訂正し暗号データブロックを出力する誤り訂正符号化部と、
前記誤り訂正符号化部が出力する前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ出力するデータ分割部と、
複数の該復号化アルゴリズムと、該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、
前記記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と、
前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部と、
前記復号化部が出力する前記復号データが音声符号化データであるか、あるいはディジタルデータであるかを判定する判定部と、
前記判定部に接続され前記ディジタルデータを外部へ出力するインタフェースとなる外部インタフェース部と、
前記判定部に接続され前記音声符号化データを復号しディジタル音声を出力する音声復号化部と、
前記音声復号化部の出力する前記ディジタル音声をアナログ化しアナログ音声を出力するアナログ変換部と、
前記アナログ変換部の出力するアナログ音声を外部に出力する音声出力部と、を有する無線通信端末。

【請求項７】アナログ音声が入力される音声入力部と、
前記音声入力部から入力される前記アナログ音声をディジタル音声信号に変換し出力するディジタル変換部と、
前記ディジタル変換部が出力する前記ディジタル音声信号を音声符号化データに音声符号化し出力する音声符号化部と、
外部ディジタルデータを入力するための外部インタフェース部と、
前記音声符号化データと前記外部ディジタルデータとのいずれか一方を選択し出力するデータ選択部と、
複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、
前記複数の暗号化アルゴリズムのうちの何れか一つを選択する暗号選択部と、
前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記データ選択部により選択されるデータを暗号化し暗号文を出力する暗号化部と、
前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし所定の識別子暗号化アルゴリズムにより暗号化し出力する識別子暗号化部と、前記識別子暗号化部が出力す

る暗号化された識別子を前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、
前記暗号データブロック生成部が出力する前記暗号データブロックに誤り訂正符号化を施し誤り訂正符号化データブロックを出力する誤り訂正符号化部と、
前記誤り訂正符号化部が出力する前記誤り訂正符号化データブロックに変調を施し変調データを出力する変調処理部と、
前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線通信端末。

【請求項８】基地局と多元接続により通信を行う通信端末において、
前記基地局が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、
前記無線受信部が取り出す変調信号に復調処理を施し誤り訂正符号化データブロックを取り出し出力する誤り復調処理部と、
前記復調処理部が出力する前記誤り訂正符号化データブロック中の誤りを検出し誤りを訂正し暗号データブロックを出力する誤り訂正符号化部と、
前記誤り訂正符号化部が出力する前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する暗号化された識別子とを取り出しそれぞれ出力するデータ分割部と、
複数の前記復号化アルゴリズムと、該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、
前記受信データ分割部から出力される前記暗号化された識別子を復号化し識別子を出力する識別子復号化部と、
前記識別子復号化部の出力する前記識別子を前記記憶部に記憶される前記復号化テーブルを参照し対応する復号化アルゴリズムを選択する復号選択部と、
前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部と、
前記復号化部が出力する前記復号データが音声符号化データであるか、あるいはディジタルデータであるかを判定する判定部と、
前記判定部に接続され前記ディジタルデータを外部へ出力するインタフェースとなる外部インタフェース部と、
前記判定部に接続され前記音声符号化データを復号しディジタル音声を出力する音声復号化部と、
前記音声復号化部の出力する前記ディジタル音声をアナログ化しアナログ音声を出力するアナログ変換部と、
前記アナログ変換部の出力するアナログ音声を外部に出力する音声出力部と、を有する無線通信端末。

【請求項９】請求項３乃至８に記載の無線通信端末において、
前記記憶部は着脱交換可能なメモリであり、予め任意の

暗号化／復号化アルゴリズムを記憶しておくことを特徴とする無線通信端末。

【請求項１０】請求項３乃至８に記載の無線通信端末において、
前記記憶部は、
予め任意の暗号化／復号化アルゴリズムが記憶される着脱交換可能な電子カードと、
前記電子カードに電源を供給し情報を送受する電子カード読取り部とを有することを特徴とする無線通信端末。

【請求項１１】暗号化／復号化を施し通信を行う無線通信端末において、
前記暗号化／復号化に用いられる少なくとも一つの暗号と該暗号の識別に用いられる暗号識別子とを記憶する着脱可能な記憶手段と、
該記憶手段を着脱交換可能に装着する装着手段と、
前記装着手段に接続され前記記憶部に記憶された情報を読み出す読出手段と、
前記読出手段を制御する制御手段と、を有することを特徴とする無線通信端末。

【請求項１２】請求項１乃至１１に記載の無線通信端末において、
前記記憶部はカード型のメモリであることを特徴とする無線通信端末。

【請求項１３】請求項１乃至１２に記載の無線通信端末において、
前記暗号化選択部に対し選択すべき暗号化アルゴリズムを指示する制御信号を発する制御手段を有することを特徴とする無線通信端末。

【請求項１４】請求項１３に記載の無線通信端末において、
前記通信端末はキー入力部を有し、
前記キー入力部から入力される入力データに基づいて前記制御部が前記制御信号を発することを特徴とする無線通信端末。

【請求項１５】入力された音声をディジタル化し暗号化し通信を行う無線通信端末において、
複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する着脱式記憶部を装着すべく成る装着部と、
前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、
前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が出力する前記音声符号化データを暗号化し暗号文を出力する暗号化部と、
前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、
前記暗号データブロック生成部が出力する前記暗号デー

タブロックに変調を施し変調データを出力する変調処理部と、
前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線通信端末。
【請求項１６】移動体通信に用いられる暗号化アルゴリズムを格納する記憶装置において、
複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する着脱式記憶装置。
【請求項１７】請求項１６に記載の着脱式記憶装置において、
前記着脱式記憶装置はカード型のメモリであることを特徴とする着脱式記憶装置。
【請求項１８】無線通信端末と通信を行なう無線基地局おいて、
記憶部を装着すべくなる装着部と、
前記装着部に着脱可能に装着され、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、
前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、
前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいてデータを暗号化し暗号文を出力する暗号化部と、
前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、
前記暗号データブロック生成部が出力する前記暗号データブロックに変調を施し変調データを出力する変調処理部と、
前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有することを特徴とする無線基地局。
【請求項１９】無線通信端末と通信を行う無線基地局において、
前記無線通信端末が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、
前記無線受信部が取り出す変調信号に復調処理を施し暗号データブロックを出力する復調処理部と、
前記復調処理部が出力する前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ出力するデータ分割部と、
複数の該復号化アルゴリズムと該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する着脱可能な記憶部と、

前記着脱式記憶部を装着する装着部と、
前記着脱式記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と、
前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部と、を有する無線基地局。
【請求項２０】請求項１８、１９のいずれかに記載の無線基地局において、
前記記憶部は着脱交換可能なメモリであり、予め任意の暗号化／復号化アルゴリズムを記憶しておくことを特徴とする無線基地局。
【請求項２１】請求項１８、１９のいずれかに記載の無線基地局において、
前記記憶部は、
予め任意の暗号化／復号化アルゴリズムが記憶されるメモリを内蔵した着脱交換可能な電子カードと、
前記電子カードに電源を供給し情報を送受する電子カード読取り部とを有することを特徴とする無線基地局。
【請求項２２】暗号化／復号化を施し通信を行う無線基地局において、
前記暗号化／復号化に用いられる少なくとも一つの暗号と該暗号の識別に用いられる暗号識別子とを記憶する着脱可能な記憶手段と、
該記憶手段を着脱交換可能に装着する装着手段と、
前記装着手段に接続され前記記憶部に記憶された情報を読み出す読出手段と、
前記読出手段を制御する制御手段と、を有することを特徴とする無線基地局。
【請求項２３】請求項１８乃至２１に記載の無線基地局において、
前記暗号化選択部に対し選択すべき暗号化アルゴリズムを指示する制御信号を発する制御手段を有することを特徴とする無線基地局。
【請求項２４】複数の無線通信端末と暗号化を施し通信を行なう無線基地局において、
複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する着脱式記憶部を装着すべく成る装着部と、
前記複数の暗号化アルゴリズムのうち前記無線通信端末が備えている暗号化アルゴリズムと共通のもののうちの何れか一つを選択する暗号選択部と、
前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が出力する前記音声符号化データを暗号化し暗号文を出力する暗号化部と、
前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する

暗号データブロック生成部と、
前記暗号データブロック生成部が出力する前記暗号データブロックに変調を施し変調データを出力する変調処理部と、
前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線基地局。

【請求項２５】無線通信端末と暗号化を施し通信を行なう無線基地局を管理する管理局において、
複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、
前記記憶部に記憶された暗号化テーブルを前記無線基地局に送信する送信部と、
前記記憶部及び送信部を制御する制御部と、を有することを特徴とする管理局。

【請求項２６】無線通信端末との暗号化通信に用いられる暗号化テーブルを所有する無線基地局を管理する管理局において、
複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、
前記記憶部に記憶される暗号化テーブルを前記無線基地局への送信と、及び、該送信された暗号化テーブルに基づいて前記無線基地局の所有する暗号化テーブルを更新するよう命令する命令信号の送信とを行なう送信部と、
前記記憶部及び送信部を制御する制御部と、を有することを特徴とする管理局。

【請求項２７】管理局によって管理され、無線通信端末と暗号化を施し通信を行なう無線基地局において、
前記管理局から送信される命令信号に基づいて、前記管理局から送信されてきた暗号化テーブルを記憶する記憶部を有することを特徴とする無線基地局。

【請求項２８】管理局に管理され、無線通信端末と通信を行う無線基地局において、
前記無線通信端末が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、
前記無線受信部が取り出す変調信号に復調処理を施し暗号データブロックを出力する復調処理部と、
前記復調処理部が出力する前記暗号データブロックから暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ出力するデータ分割部と、
複数の該復号化アルゴリズムと該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、
前記着脱式記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と、
前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部と、を有し、
前記管理局が送信する暗号化テーブルに基づいて前記記憶部に記憶される暗号化テーブルを更新することを特徴とする無線基地局。

【請求項２９】無線通信端末と通信を行なう無線基地局おいて、
複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、
前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、
前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいてデータを暗号化し暗号文を出力する暗号化部と、
前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、
前記暗号データブロック生成部が出力する前記暗号データブロックに変調を施し変調データを出力する変調処理部と、
前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有し、
前記管理局が送信する暗号化テーブルに基づいて、前記記憶部に記憶された暗号化テーブルを更新することを特徴とする無線基地局。

【請求項３０】第１の無線通信端末と第２の無線通信端末とが無線基地局を介して通信を行なう通信システムにおいて、
前記第１の無線通信端末は、
前記無線基地局との暗号化通信に用いられる第１の暗号化／復号化アルゴリズムを有し、
前記第２の無線通信端末は、
前記無線基地局との暗号化通信に用いられる第１の暗号化／復号化アルゴリズムとは異なる第２の暗号化／復号化アルゴリズムを少なくとも有し、
前記基地局は、前記第１の暗号化／復号化アルゴリズム及び第２の暗号化／復号化アルゴリズムを有することを特徴とする通信システム。

【請求項３１】第１の無線通信端末と、該第１の無線通信端末と無線通信を行なう第１の無線基地局と、該第１の無線基地局と通信を行なう第２の無線基地局と、該第２の無線基地局と無線通信を行なう第２の無線通信端末とを有する通信システムにおいて、
前記第１の無線通信端末は、
前記第１の無線基地局との暗号化通信に用いられる第１

の暗号化／復号化アルゴリズムを有し、
前記第２の無線通信端末は、
前記第２の基地局との暗号化通信に用いられる第１の暗号化／復号化アルゴリズムとは異なる第２の暗号化／復号化アルゴリズムを少なくとも有し、
前記第１の無線基地局は、
少なくとも前記第１の暗号化／復号化アルゴリズムを有し、
前記第２の無線基地局は、
少なくとも前記第２の暗号化／復号化アルゴリズムを有することを特徴とする通信システム。

【請求項３２】第１の無線通信端末と第２の無線通信端末とが無線基地局を介して通信を行なう通信システムにおいて、
前記第１の無線通信端末は、
前記無線基地局を介して前記第２の無線通信端末との暗号化通信に用いられる暗号化／復号化アルゴリズムを有し、
前記第２の無線通信端末は、
前記第１の無線通信端末との暗号化通信に用いられる前記暗号化／復号化アルゴリズムと、
前記暗号化／復号化アルゴリズムとは異なる暗号化アルゴリズムを少なくとも一つ有することを特徴とする通信システム。

【請求項３３】第１の無線通信端末と、該第１の無線通信端末と無線通信を行なう第１の無線基地局と、該第１の無線基地局と通信を行なう第２の無線基地局と、該第２の無線基地局と無線通信を行なう第２の無線通信端末とを有する通信システムにおいて、
前記第１の無線通信端末は、
前記第１の無線基地局及び前記第２の無線基地局とを介して前記第２の無線通信端末との暗号化通信に用いられる暗号化／復号化アルゴリズムを有し、
前記第２の無線通信端末は、
前記第２の無線基地局及び前記第１の無線基地局とを介して前記第１の無線通信端末との暗号化通信に用いられる前記暗号化／復号化アルゴリズムと、
前記暗号化／復号化アルゴリズムとは異なる他の暗号化／復号化アルゴリズムを少なくとも一つ有することを特徴とする通信システム。

【請求項３４】無線通信に用いられる暗号化方法において、
音声を入力し、
前記入力された音声を音声符号化して情報圧縮し、
前記情報圧縮された音声に対し暗号化を施す複数の暗号化アルゴリズムから一つを選択し、
前記選択された暗号化アルゴリズムに基づいて情報圧縮された音声を暗号化し、
前記暗号化アルゴリズムに対応する識別子を識別子暗号化し、

前記暗号化された音声と前記識別子暗号化された識別子とを一つデータへとデータブロック化し、
前記データブロック化されたデータを送信することを特徴とする暗号化方法。

【請求項３５】無線通信に用いられる復号化方法において、
受信データから暗号文と識別子暗号文を抽出分離し、
前記識別子暗号文から識別子を復号化し、
復号された識別子に基づいて前記暗号文を復号化する復号化アルゴリズムを選択し、
選択された復号化アルゴリズムで暗号文を復号化し音声圧縮情報を出力し、
前記音声圧縮情報を情報伸長し、音声を出力することを特徴とする復号化方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、通信回路や各種通信回線等を経由して情報の送受信を行う情報通信機器に応用される、暗号化／復号化装置を有する無線通信端末、無線基地局及びこれらを有する通信システムに関する。

【０００２】

【従来の技術】暗号化を施し通信を行う技術として、特表平６－５０６８１３に開示されているような暗号化通信方法がある。この暗号化通信方法では、無線機に複数の暗号化キーとそれらに対応するキー識別子とを備え、送信側無線機でキー識別子を選択し、選択されたキー識別子に対応した暗号化キーで平文を暗号化して暗号文を生成し、暗号化に用いたキー識別子と共に暗号文を相手無線機に送信し、相手無線機では、送られてきたキー識別子に基づいて暗号文を解読することが提案されている。

【０００３】一方で、携帯無線電話システムであるピー・エイチ・エス（以下ＰＨＳと称す）では、スクランブル／デスクランブル処理あるいは簡易秘話処理をもちいて通信端末と基地局の間で暗号化を行っている。

【０００４】

【発明が解決しようとする課題】上記のようにＰＨＳでは、暗号化／復号化アルゴリズムとしてスクランブルあるいは簡易秘話をもちいて暗号化処理を行い、任意の端末間あるいは、端末と基地局間で情報の伝送を行っている。

【０００５】しかし、上述したスクランブルと簡易秘話は簡略的なものであり、盗聴者によって容易に解読されうるものである。今後はセキュリティの確保が一層求められるため、暗号化アルゴリズムを公開しても解読が困難な、より強力な暗号化を行わなければならないという第一の課題がある。

【０００６】現状では、スクランブルと簡易秘話以外の暗号化はオプションであり、今後各メーカーごとに様々な暗号化アルゴリズムを備えた無線通信端末が製品化さ

れよう。このような状況下では、あるメーカーのＰＨＳ端末（既存端末）で暗号化された暗号文は、通信端末を製造するメーカーの基地局（基地局側）のみでしか復号化できない状態になりうる。すなわち、同じメーカー製の同じ暗号化アルゴリズムを備えた特定の端末と基地局間、又は特定の端末間だけでしか情報の送受信を行うことができなくなる。また、今後新しい暗号化アルゴリズムが開発され、上記と同じようにその新しい暗号化アルゴリズムを備えた特定の端末と基地局間、又は特定の端末間だけでしか情報の送受信を行うことができなくなるという第２の課題がある。情報通信の発展に伴い、このような課題が障害となることは確実である。

【０００７】本発明の目的は、移動体電話通信において強力な暗号化を有する無線通信端末を提共することにある。

【０００８】さらに本発明の他の目的は、複数の異なった暗号化／復号化アルゴリズムを備えた無線通信端末との通信を可能とし、さらに、新しい暗号化／復号化アルゴリズムが提共されたときにも、新しいアルゴリズムを記憶した着脱交換式メモリにより柔軟、かつ、容易に対処できることにある。

【０００９】

【課題を解決するための手段】本発明の無線通信端末には、装着部と、前記装着部に着脱可能に装着され、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が出力する前記音声符号化データを暗号化し暗号文を出力する暗号化部と、前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、前記暗号データブロック生成部が出力する前記暗号データブロックに誤り訂正符号化を施し誤り訂正符号化データブロックを出力する誤り訂正符号化部と、前記誤り訂正符号化部が出力する前記誤り訂正符号化データブロックに変調を施し変調データを出力する変調処理部と、前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部とを設けた。

【００１０】本発明の無線通信端末は、アナログ音声を入力する音声入力部と、前記音声入力部から入力される前記アナログ音声をディジタル音声信号に変換し出力するディジタル変換部と、前記ディジタル変換部が出力する前記ディジタル音声信号を音声符号化データに音声符号化し出力するする音声符号化部と、外部ディジタルデータを入力するための外部インタフェース部と、前記音声符号化データと前記外部ディジタルデータとのいずれか一方を選択し出力するデータ選択部と、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、前記複数の暗号化アルゴリズムのうちの何れか一つを選択する暗号選択部と、前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記データ選択部により選択されるデータを暗号化し暗号文を出力する暗号化部と、前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし所定の識別子暗号化アルゴリズムにより暗号化し出力する識別子暗号化部と、前記識別子暗号化部が出力する暗号化された識別子を前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、前記暗号データブロック生成部が出力する前記暗号データブロックに誤り訂正符号化を施し誤り訂正符号化データブロックを出力する誤り訂正符号化部と、前記誤り訂正符号化部が出力する前記誤り訂正符号化データブロックに変調を施し変調データを出力する変調処理部と、前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部とを設けた。

【００１１】また、本発明の無線通信端末は、基地局と多元接続により通信を行う通信端末において、前記基地局が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、前記無線受信部が取り出す変調信号に復調処理を施し誤り訂正符号化データブロックを取り出し出力する誤り復調処理部と、前記復調処理部が出力する前記誤り訂正符号化データブロック中の誤りを検出し誤りを訂正し暗号データブロックを出力する誤り訂正符号化部と、前記誤り訂正符号化部が出力する前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する暗号化された識別子とを取り出しそれぞれ出力するデータ分割部と、複数の前記復号化アルゴリズムと、該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、前記受信データ分割部から出力される前記暗号化された識別子を復号化し識別子を出力する識別子復号化部と、前記識別子復号化部の出力する前記識別子を前記記憶部に記憶される前記復号化テーブルを参照し対応する復号化アルゴリズムを選択する復号選択部と、前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力するする復号化部と、前記復号化部が出力する前記復号データが音声符号化データであるか、あるいはディジタルデータであるかを判定する判定部と、前記判定部に接続され前記ディジタルデータを外部へ出力するインタフェースとなる外部インタフェース部と、前記判定部に接続され前記音声符号化データを復号しディジタル音声を出力す

る音声復号化部と、前記音声復号化部の出力する前記ディジタル音声をアナログ化しアナログ音声を出力するアナログ変換部と、前記アナログ変換部の出力するアナログ音声を外部に出力する音声出力部とを設けた。

【００１２】また、本発明の無線通信端末は、前記記憶部は着脱交換可能なメモリであり、予め任意の暗号化／復号化アルゴリズムを記憶しておくことを特徴とする。

【００１３】また、本発明の無線通信端末は、前記暗号化／復号化に用いられる少なくとも一つの暗号と該暗号の識別に用いられる暗号識別子とを記憶する着脱可能な記憶手段と、該記憶手段を着脱可能に装着する装着手段と、前記装着手段に接続され前記記憶部に記憶された情報を読み出す読出手段と、前記読出手段を制御する制御手段とを設けた。

【００１４】また、本発明の着脱式記憶装置は、メモリをカード形状の筐体に納めた。

【００１５】また、本発明の無線基地局は、記憶部を装着すべくなる装着部と、前記装着部に着脱可能に装着され、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいてデータを暗号化し暗号文を出力する暗号化部と、前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、前記暗号データブロック生成部が出力する前記暗号データブロックに変調を施し変調データを出力する変調処理部と、前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部とを設けた。

【００１６】また、本発明の無線基地局は、前記無線通信端末が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、前記無線受信部が取り出す変調信号に復調処理を施し暗号データブロックを出力する復調処理部と、前記復調処理部が出力する前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ出力するデータ分割部と、複数の該復号化アルゴリズムと該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する着脱可能な記憶部と、前記着脱式記憶部を装着する装着部と、前記着脱式記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と、前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部とを設けた。

【００１７】また、本発明の無線基地局は、暗号化／復

号化に用いられる少なくとも一つの暗号と該暗号の識別に用いられる暗号識別子とを記憶する着脱可能な記憶手段と、該記憶手段を着脱交換可能に装着する装着手段と、前記装着手段に接続され前記記憶部に記憶された情報を読み出す読出手段と、前記読出手段を制御する制御手段とを設けた。

【００１８】また、本発明の無線基地局は、複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する着脱式記憶部を装着すべく成る装着部と、前記複数の暗号化アルゴリズムのうち前記無線通信端末が備えている暗号化アルゴリズムと共通のもののうちの何れか一つを選択する暗号選択部と、前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が出力する前記音声符号化データを暗号化し暗号文を出力する暗号化部と、前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、前記暗号データブロック生成部が出力する前記暗号データブロックに変調を施し変調データを出力する変調処理部と、前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部とを設けた。

【００１９】また、本発明の管理局は複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、前記記憶部に記憶された暗号化テーブルを前記無線基地局に送信する送信部と、前記記憶部及び送信部を制御する制御部とを設けた。

【００２０】また、本発明の管理局は、複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、前記記憶部に記憶される暗号化テーブルを前記無線基地局への送信と、及び、該送信された暗号化テーブルに基づいて前記無線基地局の所有する暗号化テーブルを更新するよう命令する命令信号の送信とを行なう送信部と、前記記憶部及び送信部を制御する制御部とを設けた。

【００２１】また、本発明の無線基地局は、無線通信端末が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、前記無線受信部が取り出す変調信号に復調処理を施し暗号データブロックを出力する復調処理部と、前記復調処理部が出力する前記暗号データブロックから暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ出力するデータ分割部と、複数の該復号化アルゴリズム

と該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、前記着脱式記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部とを設け、前記管理局が送信する暗号化テーブルに基づいて前記記憶部に記憶される暗号化テーブルを更新する。

【００２２】また、本発明の無線通信システムは、第１の無線通信端末は、前記無線基地局との暗号化通信に用いられる第１の暗号化／復号化アルゴリズムを有し、第２の無線通信端末は、無線基地局との暗号化通信に用いられる第１の暗号化／復号化アルゴリズムとは異なる第２の暗号化／復号化アルゴリズムを少なくとも一つ有し、無線基地局は、前記第１の暗号化／復号化アルゴリズム及び第２の暗号化／復号化アルゴリズムを有する。

【００２３】また、本発明の通信システムは第１の無線通信端末は、前記第１の無線基地局との暗号化通信に用いられる第１の暗号化／復号化アルゴリズムを有し、第２の無線通信端末は、前記第２の基地局との暗号化通信に用いられる第１の暗号化／復号化アルゴリズムとは異なる第２の暗号化／復号化アルゴリズムを少なくとも有し、第１の無線基地局は、少なくとも前記第１の暗号化／復号化アルゴリズムを有し、第２の無線基地局は、少なくとも前記第２の暗号化／復号化アルゴリズムを有する。

【００２４】また、本発明の通信システムは、第１の無線通信端末は、前記無線基地局を介して第２の無線通信端末との暗号化通信に用いられる暗号化／復号化アルゴリズムを有し、前記第２の無線通信端末は、前記第１の無線通信端末との暗号化通信に用いられる前記暗号化／復号化アルゴリズムと、前記暗号化／復号化アルゴリズムとは異なる暗号化アルゴリズムを少なくとも一つ有する。

【００２５】また、本発明の通信システムは、第１の無線通信端末は、前記第１の無線基地局及び前記第２の無線基地局とを介して前記第２の無線通信端末との暗号化通信に用いられる暗号化／復号化アルゴリズムを有し、第２の無線通信端末は、第２の無線基地局及び第１の無線基地局とを介して前記第１の無線通信端末との暗号化通信に用いられる前記暗号化／復号化アルゴリズムと、前記暗号化／復号化アルゴリズムとは異なる他の暗号化／復号化アルゴリズムを少なくとも一つ有する。

【００２６】

【作用】本発明の無線通信端末は盗聴防止のため、端末ユーザの暗号化アルゴリズム変更要求時に、キー入力等の手段によって任意に又は呼接続時毎に、位置登録時毎に、通話中チャネル切り替え時毎に、認証時毎に、予め定められた時間毎に、全くランダムに、予め定められたエリア毎に端末が暗号化アルゴリズムを切り替えるため、暗号の解読がされにくくなる。また、複数の暗号化アルゴリズムと対応する暗号化アルゴリズム識別子をメモリ等の記憶手段に格納していて、ＣＰＵ等の手段が暗号化アルゴリズム識別子のビット数に対応する乱数を任意の乱数発生器で出力し、出力された乱数を用い暗号化テーブルから暗号化アルゴリズムを選択し、暗号化アルゴリズムを切り替えてもよい。その後、前記暗号化アルゴリズムでメッセージの暗号化を行い暗号文を出力し、同時に任意の暗号化アルゴリズムで暗号化アルゴリズムを識別するための識別子を暗号化する。前記暗号文は識別子暗号文と共に受信側へ伝送される。

【００２７】本発明の無線通信端末は、送信側から伝送されてきた暗号文と識別子暗号文を受け取り、識別子暗号文を任意の復号化アルゴリズムで復号化する。復号化された識別子からどの暗号化アルゴリズムを使用しているかを判断し、対応する復号化アルゴリズムを選択する。前記復号化装置は、前記暗号化装置に対応して、複数の復号化アルゴリズムをＲＯＭ等の手段に格納していて、選択された復号化アルゴリズムを切り替え、前記復号化アルゴリズムを用いて暗号文をメッセージに復号化する。

【００２８】本発明の無線通信端末は、暗号化アルゴリズム、識別子及び暗号化テーブルを記憶する記憶部が着脱可能であるため、改めて新しい暗号化アルゴリズムが提供された場合に、新しい暗号化アルゴリズムを含めて記憶した記憶部を脱着交換すれば容易に他の暗号化アルゴリズムをサポートすることができる。

【００２９】上記のように無線通信端末を構成することによって、同じ暗号化アルゴリズムを備えた特定の端末基地局間だけでしか情報の伝送を行うことができないという課題を克服することができる。

【００３０】本発明の無線基地局は、着脱交換式の記憶部を設けることにより容易に新しい暗号化アルゴリズムを網羅することが出来る。

【００３１】また本発明の管理局は、全ての暗号化テーブルを備え、この最新の暗号化テーブルを管理下にある複数の無線基地局に対して送信すると共に、無線基地局には、無線基地局の有する記憶部内の暗号化テーブルを更新するよう命令する。

【００３２】この管理局によって、無線基地局は容易に新しい暗号化アルゴリズムにも対処できる。またこの構成であれば、着脱交換式メモリは必要ないためコスト的にも有利である。

【００３３】また、本発明の通信システムでは、通信を行なう二つの無線通信端末のうち、片方が相手方と同じ暗号化アルゴリズムを含め複数備えているので、新しい暗号化アルゴリズムを備えていない無線通信端末とも通信できる。

【００３４】また、本発明の通信システムは無線通信端

末間を仲介する無線基地局が、全ての暗号化アルゴリズムを備えることで、暗号変換部としての役割を果たすため、通信しようとする無線通信端末間で共通する暗号化アルゴリズムが存在しない場合であっても暗号化通信を可能としている。

【００３５】

【実施例】本発明の実施例についてＰＨＳを例に図を参照して説明する。

【００３６】本発明の暗号化・復号化装置を備えたＰＨＳ端末機能図を送信部と受信部に分けて説明する。図１には本発明を実施する場合の一例である無線通信端末を示す。また図２，３は無線通信端末の送信部のみを示した図である。図１、２、３に示すように、無線通信端末であるＰＨＳ端末の送信部は、音声を入力するマイクと、音声をデジタル化するＡ／Ｄ変換器と、ＡＤＰＣＭやＶＳＥＬＰまたはＰＲＥ－ＬＴＰなどの一般的な音声圧縮を行なう音声符号化部と、マイク入力あるいは外部インタフェースのいずれかを選択するｄａｔａ　ｓｅｌｅｃｔｏｒ部と、暗号化を施す暗号化部と、暗号文に識別子を付加するｄａｔａ　ｂｌｏｃｋ生成部と、誤り訂正符号化を施す誤り検出・訂正符号化部と、情報に対して各種変調方式により多重変調等を行なう変調部及び無線部と、外部からのデータ入力部と成るＲＳ２３２Ｃなどの外部インタフェース部と、暗号化に用いられる暗号化アルゴリズムを選択する暗号ｓｅｌｅｃｔｏｒ部と、ユーザの希望によってキーを押すことで他の暗号化アルゴリズムに切り替えるためのキー入力を行なうキー入力部と、及び全体を司る制御部と、暗号化アルゴリズムやこの暗号化アルゴリズムの一つ一つに対応する暗号化識別子、及び暗号化アルゴリズム、識別子および暗号化アルゴリズムと識別子との関係を表わす、例えば図４に示したような暗号化テーブルを記憶する記憶部を有して構成される。ここで、制御部は一つであっても複数個備え各処理及び制御を分担してもよい。また、暗号化アルゴリズムと識別子は必ずしも一対一でなくてもよい。というのは、複数の暗号化アルゴリズムを組み合わせて一つの暗号化を施す場合など、複数ある暗号化アルゴリズムの実行順序の関係を識別子をもちいて記述し、テーブルかして記憶すれば、既存の暗号化アルゴリズムを自由に、かつ簡単に組み合わせるだけでより強固な暗号化アルゴリズムを提供できるのである。

【００３７】また記憶部は、一つであっても複数であってもよい。ところで、新たな暗号化アルゴリズムが提案されたときに、すばやく対処できるようにするために、記憶部を着脱式にしておき、ユーザが新しい暗号化アルゴリズムが記憶されたメモリカードを自由に購入し、交換してもよい。また、着脱式でなくとも、書替え可能なメモリであってもよい。この場合、ユーザは端末のサービスセンタで書き替えてもよいし、電話回線を通じて通信によりダウンロードしてもよい。ダウンロードの場合、ユーザはキー操作によって制御部に暗号化アルゴリズムをダウンロードする旨を指定し、制御部は電話回線より送られてきた暗号化アルゴリズムと識別子などを記憶部のテーブルに追加書き込みする。

【００３８】次に、これらの構成による端末の具体的な信号処理手順を図５に示すフローチャートを参照して説明する。

【００３９】まず、ステップ８００において、伝送したい音声データをマイク等の手段で又、ＦＡＸ、パソコン等の３２ｋｂｐｓデータをインタフェースコネクタ等の外部入力端子から入力する。次に、ステップ８０１において、ｄａｔａ　ｓｅｌｅｃｔｏｒ部で音声データがＰＨＳ端末に入力されるか判定を行う。音声データが入力されるならばステップ８０２以降の処理を行い、ＦＡＸ、パソコン等の３２ｋｂｐｓデータが入力されるならばステップ８０４以降の処理を行う。次に、ステップ８０２において、ディジタル処理を行うために、入力された３００～３４００Ｈｚのアナログ音声信号をＡ／Ｄ変換器でディジタル信号に変換する。次に、ステップ８０３において、音声符号化部で音声符号化処理を行い、６４ｋｂｐｓのＰＣＭデータを３２ｋｂｐｓの音声符号化ビットに変換する。次に、ステップ８０４において、ユーザが任意にキーパッド等の手段で暗号化アルゴリズム識別子を入力する。次に、ステップ８０５において、制御部ではキー入力された暗号化アルゴリズム識別子をスキャンして読みとる。記憶部は、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する暗号化アルゴリズム識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルを備えていて、ステップ８０６において、暗号ｓｅｌｅｃｔｏｒ部は制御部で読みとった暗号化アルゴリズム識別子に基づき対応する暗号化アルゴリズムを選定する。次に、ステップ８０７において、暗号化部で前記音声符号化ビットやＦＡＸ、パソコン等の各種データに対して、任意のビット長だけ格納し、そのビット長を１ブロックとして暗号ｓｅｌｅｃｔｏｒ部で選定された暗号化アルゴリズムで暗号化処理を行う。次に、ステップ８０８において、ｄａｔａ　ｂｌｏｃｋ生成部で、暗号化アルゴリズム識別子と暗号化されたビットをあるブロック（ＰＨＳの場合はデータ１６０ビット）毎に格納し、そのブロックごとに誤り検出・訂正符号化部で巡回符号（ＣＲＣ）による符号化を行い、データ１６０ビットに符号化されたビットを付け加えるチャネルコーデック処理を行う。次に、ステップ８０９において、変調部でチャネルコーデック処理によって出力された送信データのディジタル変調（ＰＨＳの場合はπ／４シフトＱＰＳＫ）を行う。次に、ステップ８１０において、無声部で無線チャネルの設定を行い、音声や各種データを無線回線を使って伝送することができる。以上の処理によって、音声や各種データを無線回線を使って送信すること

ができる。

【００４０】次に受信時の処理について説明する。図１、図６及び図７にはＰＨＳ端末の受信部を示している。本発明の無線通信端末の実施例では、音声を出力するスピーカと、デジタル信号をアナログ信号にするＤ／Ａ変換器と、音声圧縮された信号を復号する音声復号化部と、送られてきた暗号文を復号する復号化部と、送られてきた信号から識別子と暗号文とを分離し出力するｄａｔａ分割部と、誤り検出や誤り訂正を施す誤り検出・訂正部と、送られてきた信号を復調する復調部及び無線部と、ＲＳ２３２Ｃ等のインタフェースや文字表示装置である外部インタフェースと、識別子に基づいて暗号文を復号するための復号化アルゴリズムを選択する復号ｓｅｌｅｃｔｏｒ部と、全体を統括する制御部と、復号化アルゴリズムや復号化テーブルを記憶する記憶部を有している。

【００４１】受信部の処理手順を図８に示し、該フローチャートを参照して処理手順について説明する。受信部では、まずステップ９００において無線部で無線チャネルから伝送されてきた信号を受け取る。次に、ステップ９０１において、復調部で信号の復調処理を行う。次に、ステップ９０２において、誤り検出・訂正部で送信部と同じように復調処理を行ったビットに対して、あるブロック（ＰＨＳの場合はデータ１６０ビット）毎に、巡回符号（ＣＲＣ）による符号化を行い、送信部から伝送されてきた巡回符号（ＣＲＣ）による符号化ビットと比較し、伝送路での誤り検出を行う。次に、ステップ９０３において、伝送路での誤りが検出されたかどうかの判定を行う。誤りが検出されればステップ９０４の処理を行い、誤りが検出されなければステップ９０５の処理を行う。次に、ステップ９０４において、誤り除去又は低減処理を行う。次に、ステップ９０５において、ｄａｔａ分割部で暗号文と暗号化アルゴリズム識別子を分割する。記憶部は、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する暗号化アルゴリズム識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルを備えていて、ステップ９０６において、復号ｓｅｌｅｃｔｏｒ部は、受信した暗号化アルゴリズム識別子に基づき対応する暗号化アルゴリズムを選定する。次に、ステップ９０７において、復号化部で情報ビット（ＰＨＳの場合は１６０ビット）に対して、任意のビット長だけ格納し、そのビット長を１ブロックとして復号ｓｅｌｅｃｔｏｒ部で選定された復号化アルゴリズムで復号化処理を行う。次に、ステップ９０８において、ｄａｔａ判定部で音声データであるか判定を行う。音声データであればステップ９０９へ、ＦＡＸ、パソコン等の３２ｋｂｐｓデータであればステップ９１０の処理を行う。次に、ステップ９１１において、音声復号化部で音声復号化処理を行い、音声符号化ビットをディジタル信号に変換する。次に、ステップ９１２において、アナログ信号を得るために（音声を出力するため）、Ｄ／Ａ変換器でディジタル信号を３００～３４００Ｈｚのアナログ音声に変換する。次に、ステップ９１３において、スピーカ等の手段を通して、音声を出力する。また、ステップ９１４において、ＦＡＸ、パソコン等の３２ｋｂｐｓデータをインタフェースコネクタ等の外部入力端子から出力する。以上の処理によって、無線回線から音声や各種データを受信することができる。

【００４２】次に、本発明の暗号化・復号化装置を備えた基地局の機能図を送信機能と受信機能について説明する。図９，１０にはとりわけ送信部を，図１１，１２には受信部を示している。基地局の送信機能としては、ＤＳＵ（ディジタル・サービス・ユニット）と、ＳＩＮＦと、エコーキャンセラと、音声符号化部と、暗号化部と、ｄａｔａ　ｂｌｏｃｋ生成部と、誤り検出・訂正符号化部と、変調部と、無線部と、暗号ｓｅｌｅｃｔｏｒ部と、制御部と、記憶部を有して構成される。送信機能としては、まず、ＰＢＸから送られてきた２Ｂ＋Ｄ（Ｂ：６４ｋｂｐｓ，Ｄ：１６ｋｂｐｓ）の信号がＤＳＵを介して基地局に入る。次に、ＳＩＮＦ（Ｓ－Ｉｎｔｅｒｆａｃｅ）で２Ｂ＋Ｄの信号をＢチャネル（情報信号）２つとＤチャネル（制御信号）に分割する。次に、エコーキャンセラで、回線系エコー（２線－４線変換のハイブリッドでの不整合によるエコー）の消去を行う。次に、音声符号化部で音声符号化処理を行い、６４ｋｂｐｓのディジタル信号を３２ｋｂｐｓのデータに変換する。次に、暗号化アルゴリズム識別子のビット数に対応する乱数を任意の乱数発生器で出力する。記憶部は、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する暗号化アルゴリズム識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルを備えていて、暗号ｓｅｌｅｃｔｏｒ部は、乱数発生器で出力された暗号化アルゴリズム識別子に基づき対応する暗号化アルゴリズムを選定する。次に、暗号化部で前記３２ｋｂｐｓのデータに対して、任意のビット長だけ格納し、そのビット長を１ブロックとして暗号ｓｅｌｅｃｔｏｒ部で選定された暗号化アルゴリズムで暗号化処理を行う。次に、ｄａｔａ　ｂｌｏｃｋ生成部で暗号化アルゴリズム識別子と暗号化されたビットをあるブロック（ＰＨＳの場合はデータ１６０ビット）毎に格納し、そのブロックごとに誤り検出・訂正符号化部で巡回符号（ＣＲＣ）による符号化を行い、データ１６０ビットに符号化されたビットを付け加えるチャネルコーデック処理を行う。次に、変調部でチャネルコーデック処理によって出力された送信データのディジタル変調（ＰＨＳの場合はπ／４シフトＱＰＳＫ）を行う。次に、無声部で無線チャネルの設定を行い、音声や各種データを無線回線を使って伝送することができる。以上の処理によって、音声や各種データを無線回線を使

って送信することができる。

【００４３】受信機能としては、ＤＳＵと、ＳＩＮＦと、エコーキャンセラと、音声復号化部と、復号化部と、ｄａｔａ分割部と、誤り検出・訂正部と、復調部と、無線部と、復号ｓｅｌｅｃｔｏｒ部と、制御部と、記憶部を有して構成される。受信時の動作を以下に説明する。受信部では、無線部で無線チャネルから伝送されてきた信号を受け取る。次に、復調部で信号の復調処理を行う。次に、誤り検出・訂正部で送信部と同じように復調処理を行ったビットに対して、あるブロック（ＰＨＳの場合はデータ１６０ビット）毎に、巡回符号（ＣＲＣ）による符号化を行い、送信部から伝送されてきた巡回符号（ＣＲＣ）による符号化ビットと比較し、伝送路での誤り検出を行う。次に、伝送路での誤りが検出されたかどうかの判定を行う。誤りが検出されれば、誤り除去又は低減処理を行う。次に、ｄａｔａ分割部で暗号文と暗号化アルゴリズム識別子を分割する。記憶部は、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する暗号化アルゴリズム識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルを備えていて、復号ｓｅｌｅｃｔｏｒ部は、受信した暗号化アルゴリズム識別子に基づき対応する暗号化アルゴリズムを選定する。次に、復号化部で情報ビット（ＰＨＳの場合は１６０ビット）に対して、任意のビット長だけ格納し、そのビット長を１ブロックとして復号ｓｅｌｅｃｔｏｒ部で選定された復号化アルゴリズムで復号化処理を行う。次に、音声復号化部で音声復号化処理を行い、音声符号化ビットをディジタル信号に変換する。次に、エコーキャンセラで、音響系エコー（スピーカーマイク間のエコー）の消去を行う。次に、ＳＩＮＦで、Ｂチャネル（情報信号）２つとＤチャネル（制御信号）をまとめて２Ｂ＋Ｄの信号を生成する。２Ｂ＋Ｄの信号はＤＳＵを介してＰＢＸへ伝送される。以上の処理によって、無線回線から音声や各種データを受信し、ＰＢＸへデータ伝送をすることができる。

【００４４】ＧＳＭ、ＦＰＬＭＴＳについてもこの構成で十分である。

【００４５】図１３は、本発明にかかるＰＨＳの他の実施例を示している。

【００４６】ＰＨＳは、事業所用と屋外用（公衆用）と家庭用に分かれている。事業所用ＰＨＳは、ディジタルコードレス端末３００と、事業所内基地局３０１と、事業所用ＰＢＸ３０２を有して構成される。屋外用（公衆用）ＰＨＳは、ＰＨＳ端末３０３～３０４と、屋外基地局３０５と、モジュールアダプタ３０６を有して構成される。

【００４７】家庭用ＰＨＳは、ＰＨＳ端末３０７と、家庭内基地局３０８を有して構成される。それぞれのシステムは、交換機を介して一般電話機３１０や他の通信機器と接続される。本発明の暗号化／復号化部は、図に示すようにそれぞれのシステムの端末、基地局内、又はＰＢＸ内に含まれている。

【００４８】次に、ＰＨＳ端末機能図を図１４を参照して説明する。

【００４９】ＰＨＳ端末は、全体の制御を行う制御部４００と、制御データ及び制御手順等を記憶する記憶部４０１と、キー入力を行うキーパッド４０２と、表示出力を行うディスプレイ４０３と、着信音等を出力するサウンダ４０４と、これら入出力部と制御部との間のインターフェース部４０５と、無線回路部４０６と、ベースバンド処理部４０７、マイク４０８と、スピーカ４０９を有して構成される。

【００５０】次に、図１５のＰＨＳ端末のブロック図と図１６、１７のＰＨＳ送信部／受信部のフローチャートを参照して処理手順について説明する。ＰＨＳ端末は、図１４のベースバンド処理部４０７に対応するリニアコーデック処理部５１０と、音声符号化／復号化部５１１と、音声／３２ｋｂｐｓデータ切替部５１２と、暗号化／復号化部５１３と、チャネルコーデック処理部５１４と、モデム処理部５１５と、図１４の無線回路部４０６に対応する無線回路部５１６を有して構成される。送信部は、まず、ステップ６００において、伝送したい音声／３２ｋｂｐｓデータを入力する。次に、ステップ６０１において、音声／３２ｋｂｐｓデータ切替部５１２で音声データがＰＨＳ端末に入力されるか判定を行う。音声データが入力されるならばステップ６０２以降の処理を行い、３２ｋｂｐｓデータが入力されるならばステップ６０４以降の処理を行う。次に、ステップ６０２において、ディジタル処理を行うために、入力された３００～３４００Ｈｚのアナログ音声信号をリニアコーデック処理部５１０で６４ｋｂｐｓのディジタル信号に変換する。次に、ステップ６０３において、音声符号化／復号化部４１１で音声符号化処理を行い、６４ｋｂｐｓのＰＣＭデータを３２ｋｂｐｓの音声符号化ビットに変換する。次に、ステップ６０４において、暗号化／復号化処理部５１３で前記音声符号化データやＦＡＸ、パソコン等の各種データに対して、任意のビット長だけ格納し、そのビット長を１ブロックとして任意の暗号化アルゴリズムで暗号化処理を行う。次に、ステップ６０５において、チャネルコーデック処理部５１４で暗号化されたビットをあるブロック（ＰＨＳの場合はデータ１６０ビット）毎に格納し、そのブロックごとに巡回符号（ＣＲＣ）による符号化を行い、データ１６０ビットに符号化されたビットを付け加えるチャネルコーデック処理を行う。次に、ステップ６０６において、モデム処理部５１５でチャネルコーデック処理によって出力された送信データのディジタル変調（ＰＨＳの場合はπ／４シフトＱＰＳＫ）を行う。次に、ステップ６０７において、無声回路部５１６で無線チャネルの設定を行い、音声や各種データを無線回線を使って伝送することができる。以上

の処理によって、音声や各種データを無線回線を使って送信することができる。

【００５１】受信時の動作を以下に説明する。受信部では、まずステップ７００において無線回路部５１６で無線チャネルから伝送されてきた信号を受け取る。次に、ステップ７０１において、モデム処理部５１５で信号の復調処理を行う。次に、ステップ７０２において、チャネルコーデック処理部５１４で送信部と同じように復調処理を行ったビットに対して、あるブロック（ＰＨＳの場合はデータ１６０ビット）毎に、巡回符号（ＣＲＣ）による符号化を行い、送信部から伝送されてきた巡回符号（ＣＲＣ）による符号化ビットと比較し、伝送路での誤り検出を行う。次に、ステップ７０３において、伝送路での誤りが検出されたかどうかの判定を行う。誤りが検出されればステップ７０４の処理を行い、誤りが検出されなければステップ７０５の処理を行う。次に、ステップ７０４において、誤り除去又は低減処理を行う。次に、ステップ７０５において、暗号化／復号化処理部５１３で情報ビット（ＰＨＳの場合は１６０ビット）に対して、任意のビット長だけ格納し、そのビット長を１ブロックとして任意の復号化アルゴリズムで復号化処理を行う。次に、ステップ７０６において、音声／３２ｋｂｐｓデータ切替部５１２で音声データであるか判定を行う。音声データであればステップ７０５へ、３２ｋｂｐｓデータであればステップ７０８の処理を行う。次に、ステップ７０７において、音声符号化／復号化部５１１で音声復号化処理を行い、３２ｋｂｐｓの音声符号化データを６４ｋｂｐｓのＰＣＭデータに変換する。次に、ステップ７０８において、アナログ信号を得るために（音声を出力するため）、リニアコーデック処理部５１０で６４ｋｂｐｓのディジタル信号を３００～３４００Ｈｚのアナログ音声に変換する。次に、ステップ７０７において、スピーカ４０２等の手段を通して、音声を出力する。また、ステップ７０８において、ＦＡＸ、パソコン等の３２ｋｂｐｓデータ５０３を出力する。以上の処理によって、無線回線から音声や各種データを受信することができる。

【００５２】また、図１５のＰＨＳ端末ブロック図中の暗号化／復号化部５１３の中の暗号化部の従来例について図１８に示し、図１９の暗号化部の処理手順と合わせて従来の暗号化部について説明する。

【００５３】暗号化部は、メッセージ格納バッファ１０１０と、暗号化アルゴリズム格納部１０１１と暗号化処理部１０１２を有して構成される。まず、ステップ１１００において、メッセージ１０００（音声符号化ビット）を入力する。次に、ステップ１１０１において、暗号化アルゴリズムの処理ビット数に応じたメッセージを１ブロックとしてメッセージ格納バッファ１０１０に格納する。次に、ステップ１１０２において、１ブロック毎に暗号化アルゴリズム格納部１０１１に格納してある暗号化アルゴリズムに基づき暗号化処理を行う。次に、ステップ１１０３において、暗号文１００１が出力される。以上の処理によって、メッセージの暗号化が行われる。

【００５４】これに対して、図１５のＰＨＳ端末ブロック図の暗号化／復号化部５１３の中の復号化部の従来例を図２０に示し、図２１の復号化部の処理手順と合わせて従来の復号化部について説明する。

【００５５】復号化部は、暗号文格納バッファ１２１０と、復号化アルゴリズム格納部１２１１と、復号化処理部１２１２を有して構成される。まず、ステップ１３００において、暗号文を入力する。次に、ステップ１３０１において、復号化アルゴリズムの処理ビット数に応じて、暗号文数ビットを１ブロックとして暗号文格納バッファ１２１０に格納する。次に、ステップ１３０２において、１ブロック毎に復号化アルゴリズム格納部に格納してある復号化アルゴリズムに基づき復号化処理を行う。次に、ステップ１３０３において、メッセージ１２０１が出力される。以上の処理によって、暗号文の復号化が行われる。

【００５６】図２２は、本発明にかかる暗号化部即ち暗号化処理を行う手段の構成図である。

【００５７】暗号化処理は、メッセージ格納バッファ１４１０と、暗号化アルゴリズム格納部１４１１－１～１４１１－Ｎと、暗号化アルゴリズム切替部１４１２と、暗号化アルゴリズム識別子決定部１４１３と、暗号化処理部１４１４と、識別子暗号化処理部１４１５と、送信データ格納部１４１６を有して構成される。メッセージ格納バッファ１４１０は、暗号化アルゴリズムの処理ビット数に応じて、メッセージ１４００を格納するバッファである。暗号化アルゴリズム格納部１４１１－１～１４１１－Ｎは、複数の暗号化アルゴリズムを全て備えていて、暗号化処理部１４１４からの命令に応じ暗号化アルゴリズムを呼び出すときに使われる手段である。暗号化アルゴリズム切替部１４１２は、盗聴防止のため、端末ユーザの暗号化アルゴリズム変更要求時に、キー入力等の手段によって任意に又は呼接続時毎に、位置登録時毎に、通話中チャネル切り替え時毎に、認証時毎に、予め定められた時間毎に、全くランダムな時間毎に、予め定められたエリア毎に端末が暗号化アルゴリズムを切り替える手段である。暗号化アルゴリズムを切り替える手段の一例としては、暗号化装置が、図４に示すように複数の暗号化アルゴリズムと対応する暗号化アルゴリズム識別子をメモリ等の手段に格納していて、ＣＰＵ等の手段が暗号化アルゴリズム識別子のビット数に対応する乱数を任意の乱数発生器で出力し、出力された乱数を用い図１４に示すような対応表から暗号化アルゴリズムを選択し、暗号化アルゴリズムを切り替える。暗号化アルゴリズム識別子決定部１４１３は、決定された暗号化アルゴリズムの識別子を出力する手段である。暗号化処理部

１４１４は、切り替えられ選択された暗号化アルゴリズムによって、メッセージを暗号化し、暗号文１４０２を出力する手段である。識別子暗号化処理部１４１５は、前記暗号化アルゴリズム識別子を任意の暗号化アルゴリズムで暗号化を行い、識別子暗号文を出力する手段である。送信データ格納部１４１６は、前記識別子暗号文１４０３と、前記暗号文１４０２を並べて同時に格納する手段である。

【００５８】ここで、対応する暗号化部の処理手順を図２３に示し、該フローチャートを参照して処理手順について説明する。

【００５９】まず、ステップ１５１０において、ユーザがキー入力で任意に暗号化アルゴリズムの変更をできるように設定するか判定を行う。もし、設定するならばステップ１２１２の処理を行い、設定しなければステップ１５１１の処理を行う。次に、ステップ１５１１において、盗聴防止のため、呼接続時毎に、位置登録時に、通話中チャネル切り替え時毎に、認証時毎に、予め定められた時間毎に、全くランダムな時間毎に、予め定められたエリア毎に端末が暗号化アルゴリズムを変更できるように設定するか判定を行う。もし設定するならば、ステップ１５１４の処理を行い、設定しなければ、ステップ１５１５の処理を行う。

【００６０】次に、ステップ１５１２において、ユーザがキー入力で暗号化アルゴリズムの変更を要求しているか判定を行う。もし変更を要求していれば、ステップ１５１４の処理を行い、変更を要求していなければステップ１５１３の処理を行う。次に、ステップ１５１３において、呼接続時又は位置登録時又は通話中チャネル切り替え時又は認証時又は予め定められた時間又は端末がエリア変更を行ったか判定を行う。１つでもあてはまれば、ステップ１５１４の処理を行い、１つもあてはまらなければ、ステップ１５１５の処理を行う。次に、ステップ１５１４において、暗号化アルゴリズム識別子のビット数に対応する乱数を任意の乱数発生器で出力し、図４に示すような対応表から暗号化アルゴリズムを決定する。なお、図４の識別子は、３ビットで示しているが、ビット数は任意で良い。ステップ１５１５においては、以前に使っていた暗号化アルゴリズムを使用する。同様に、以前に使っていた暗号化アルゴリズム識別子を使用する。次に、ステップ１５１６において、暗号化アルゴリズム識別子を任意の暗号化アルゴリズムで暗号化し、識別子暗号文１５０３を出力する。次に、ステップ１５１７において、暗号化処理の入力に応じて、メッセージ１５００の数ビットを１ブロックとして格納する。次に、ステップ１５１８において、１ブロック毎に暗号化アルゴリズムに基づき暗号化処理を行い、暗号文を前記バッファへ出力する。次に、ステップ１５１９において、前記バッファに格納された暗号文と識別子暗号文を通信用物理スロットを使って同時に伝送路へ送る。

【００６１】以上の処理によって、メッセージの暗号化が行われ、バッファへ出力された暗号文と識別子暗号文は、同時に伝送される。

【００６２】これに対して、図２４は、本発明にかかる実施例における、暗号文の復号化処理を行う手段の構成図である。

【００６３】復号化処理は、受信データ分割部１６１０と、識別子復号化処理部１６１１と、復号化アルゴリズム選択部１６１２と、復号化アルゴリズム格納部１６１３－１～１６１３－Ｎと、復号化アルゴリズム切替部１６１４と、暗号文格納バッファ１６１５と、復号化処理部１６１６を有して構成される。受信データ分割部１６１０は、受信したデータを識別子暗号文１６００と暗号文１６０１に分割する手段である。識別子復号化処理部１６１１は、前記識別子暗号文１６００の復号化を行い、暗号化アルゴリズム識別子を出力する手段である。復号化アルゴリズム選択部１６１２は、暗号化アルゴリズム識別子から図４に示すような対応表から復号化アルゴリズムを選定する手段である。復号化アルゴリズム格納部１６１３－１～１６１３－Ｎは、複数の復号化アルゴリズムを全て備えていて、復号化処理部１６１６の命令に応じ復号化アルゴリズムを呼び出すときに使われる。復号化アルゴリズム切替部１６１４は、復号化アルゴリズムを切り替える手段である。復号化処理部１６１６は、切り替えられた復号化アルゴリズムによって、メッセージ１６０３を復号化する手段である。

【００６４】ここで、対応する復号化部の処理手順を図２５に示し、該フローチャートを参照して処理手順について説明する。

【００６５】まず、ステップ１７１０において、復号化部が処理開始可能なスタンバイ状態であることを確認する。スタンバイ状態であれば、ステップ１７１１の処理を行い、スタンバイ状態でなければ、ステップ１７１０の処理を繰り返す。次に、ステップ１７１１において、受信したデータを暗号文と識別子暗号文に分割する。暗号文はステップ１７１５以降で使われ、識別子暗号文はステップ１７１２以降で使われる。次に、ステップ１７１２において、前記識別子暗号文を任意の復号化アルゴリズムで復号化し、暗号化アルゴリズム識別子を出力する。次に、１７１３において、前記暗号化アルゴリズム識別子に基づいて、図１０に示すような対応表から復号化アルゴリズムを選びだす。次に、ステップ１７１４において、選びだされた復号化アルゴリズムに切り替える。次に、ステップ１７１５において、復号化処理の入力に応じて、暗号文数ビットを１ブロックとして格納する。次に、ステップ１７１６において、１ブロック毎に復号化アルゴリズムに基づき復号化処理を行い、メッセージを出力する。

【００６６】以上の処理によって、暗号文の復号化が行われる。

【００６７】ここで、送信側から受信側への暗号化アルゴリズム識別子の伝送手段を説明する。

【００６８】暗号化アルゴリズム識別子は、端末ユーザの暗号化アルゴリズム変更要求時にキー入力で又は呼接続時毎、位置登録時毎、通話中チャネル切り替え時毎、認証時毎、予め定められた時間毎、全くランダムな時間毎、予め定められたエリア毎に暗号化アルゴリズムを変更するように設定した場合、暗号化アルゴリズムを変更する毎に送信側から受信側へ伝送する必要がある。

【００６９】呼接続時は、通話開始時のことを示し、呼接続毎に暗号化アルゴリズムを変更するように設定した場合、通話開始後すぐに暗号化アルゴリズム識別子を伝送する。位置登録は、移動局が基地局へ新たに位置登録を要求するために行うものである。位置登録時毎に暗号化アルゴリズムを変更するように設定した場合、位置登録終了後すぐに暗号化アルゴリズム識別子を伝送する。通話中チャネル切り替えは、ユーザがチャネル切り替えを要求した場合、又は受信レベルが劣化したり、受信品質が劣化した場合他のチャネルへ切り替えるものであり、ハンドオーバーも含まれる。通話中チャネル切り替え時毎に暗号化アルゴリズムを変更するように設定した場合、チャネル切り替え終了後すぐに暗号化アルゴリズム識別子を伝送する。認証時は、呼接続時、位置登録時、通話中チャネル切り替え時毎に基地局が移動局の正当性を確認するために行う。認証時毎に暗号化アルゴリズムを変更するように設定した場合、通話開始後すぐに暗号化アルゴリズム識別子を伝送する。予めフレーム（５ｍｓ）毎又は１時間毎に暗号化アルゴリズムを変更するように設定した場合、暗号化アルゴリズム変更と同時に暗号化アルゴリズム識別子を伝送する。全くランダムな時間毎に暗号化アルゴリズムを変更するとは、乱数発生器の出力の値をランダムな時間と考え、そのランダムな時間毎に暗号化アルゴリズムを変更することを示す。この場合も暗号化アルゴリズム変更と同時に暗号化アルゴリズム識別子を伝送する。

【００７０】暗号化アルゴリズム識別子を伝送する一例を以下に述べる。図２６は、本発明にかかる、低速付随チャネル（以下ＳＡＣＣＨという。）を使って暗号化アルゴリズム識別子を伝送する手段の通信用物理スロットの例を示す。図２６の暗号通信の可能な通信用物理スロットの例を示す。Ｒは信号の過渡応答を保護するための過渡応答用ランプタイム領域であり、ＳＳはフレームの信号を知らせるスタートシンボル領域であり、ＰＲはビット同期確立のためのプリアンプル領域であり、ＵＷは制御用物理スロットと通信用物理スロットを区別するための同期ワード領域であり、ＣＩはチャネルの種別を規定するチャネル種別領域であり、ＳＡは制御情報領域と該制御情報領域内に格納される情報の種類の識別符号である識別符号領域とから構成されるＳＡＣＣＨ領域であり、ＴＣＨは伝送すべき情報を格納すべき情報を格納する情報チャネル領域であり、ＣＲＣは誤り検出用巡回符号領域であり、ガードビット領域は送信バースト信号が隣接するスロット間で相互に衝突しないようにバースト信号間に用意する無信号時間である。上記制御情報領域内に格納される情報は暗号化及び復号化の同期確保用情報出ある。

【００７１】暗号化及び復号化間の同期確保用の暗号化情報領域と、伝送すべき情報を格納する情報チャネル領域と、通話中、ＳＡＣＣＨを使用するのは、位置登録、チャネル切り替えの時であり、それ以外では使用されていない。よって、使用されていない時に、暗号化アルゴリズム識別子をＳＡＣＣＨを使って暗号化側から復号化側へ伝送すれば、同期はずれを防止できる。

【００７２】ここで、対応する暗号化アルゴリズム識別子の送信手順を図２７に示し、該フローチャートを参照して処理手順について説明する。まず、ステップ１９００で低速付随チャネルが使用可能な状態であるか判定を行う。使用可能な状態は、ＳＡＣＣＨの先頭ビットが２スロット連続で１の場合であり、使用不可能な状態はＳＡＣＣＨの先頭ビットが１スロット目が０で、２スロット目が１の場合である。もし、使用可能な状態であればステップ１９０１の処理を行い、使用不可能な状態であればステップ１９０４の処理を行う。ステップ１９０１で暗号化アルゴリズム識別子を伝送していることを示す識別子を付ける。識別子は、ＳＡＣＣＨの先頭ビットが２スロット連続で０の場合とする。次に、ステップ１９０２で、暗号化アルゴリズム識別子をＳＡＣＣＨの情報フィールドに入力する。ステップ１９０３では、そのフレームに関して暗号化アルゴリズム識別子の伝送を行わない。

【００７３】また、暗号化アルゴリズム識別子の受信手順を図２８に示し、該フローチャートを参照して、処理手順について説明する。まず、ステップ２０００で、ＳＡＣＣＨが暗号化アルゴリズム識別子情報であるかを判定する。暗号化アルゴリズム識別子情報である場合は、ＳＡＣＣＨの先頭ビットが２スロット連続で０の場合であり、それ以外の場合は暗号化アルゴリズム識別子情報でない。暗号化アルゴリズム識別子情報でない場合はステップ２００２の処理を行い、暗号化アルゴリズム識別子の場合は、ステップ２００１の処理を行う。ステップ２００１では、ＳＡＣＣＨの情報フィールドから暗号化アルゴリズム識別子を受け取る。ステップ２００２では、ＳＡＣＣＨの情報フィールドから暗号化アルゴリズム識別子を受け取らない。以上の処理によって、ＳＡＣＣＨ使用可能なときのみ、暗号化アルゴリズム識別子の送受信を行うことができる。

【００７４】今後新しい暗号化アルゴリズムが開発され、その新しい暗号化アルゴリズムを備えた特定の端末と基地局間、又は特定の端末間だけしか情報の送受信を行うことができなくなるという課題を解決するために次

のような着脱式メモリシステムを利用した暗号化／復号化装置の構成図を図２９及び図１に示し、該構成図を参照して実施例を説明する。

【００７５】本発明による着脱式メモリシステムは、各種端末機器２１１０と、着脱式メモリ読取り装置２１１１と、着脱式メモリ２１１２を有して構成される。

【００７６】なお、着脱式メモリ内部は、例えばＤＳＰ、ＣＰＵ、ＲＯＭ、ＲＡＭ各種ＣＭＯＳ等の一般的な電子デバイスにて構成される。

【００７７】各種端末機器２１１０としては、パーソナルコンピュータ・自動取引装置（ＡＴＭ）やＰＨＳ端末など応用分野のニーズに対応した各種の装置が開発されている。

【００７８】着脱式メモリ読取り装置２１１１は、着脱式メモリ２１１２の動作に必要な電源２１００、クロック等の制御信号２１０１を供給し、データ２１０２の送受信の制御を行うユニットであり、各種端末機器あるいはホストシステムに接続することができてもよい。

【００７９】着脱式メモリ２１１２の例としては、ＲＡＭあるいはＲＯＭ等の素子を高密度実装技術により内蔵したものである。また、読取り装置はマイクロコンピュータの制御プログラムの管理下で装着部に設けられた接点を通して外部装置との情報交換を行う。着脱式メモリに内臓されたメモリ２１２２は、データ保護のため、一定の手順で処理が行われた場合のみアクセスされるよう制御されている。

【００８０】ここで、本発明の着脱式メモリシステムの処理手順を図３０に示し、該フローチャートを参照して、処理手順について説明する。

【００８１】まず、ステップ２２００において、着脱式メモリを各種端末機器に接続された着脱式メモリ読取り装置に差し込む。次に、ステップ２２０１において、着脱式メモリ読取り装置を通じ、着脱式メモリに電源、クロック、制御信号が供給される。次に、ステップ２２０２において、あらかじめ決められたプロトコルに基づきメモリに格納されている暗号化アルゴリズムを読み取る。

【００８２】以上の処理によって、各種端末機器に接続された着脱式メモリ読取り装置が、着脱式メモリ上の接点を通じて情報のやりとりを行う。

【００８３】図３１は、本発明の着脱式メモリシステムを利用した暗号化装置の実施例であり、着脱式メモリのリード／ライトを行う着脱式メモリ読取り装置用のスロットを持つ暗号化／復号化装置を備えたＰＨＳ端末を示す。

【００８４】本発明によるＰＨＳ端末は、ＰＨＳ端末本体２３００と、着脱式メモリ読取り装置２３０１と、着脱式メモリ２３０２を有して構成される。

【００８５】ＰＨＳ端末本体２３００は、音声データやＦＡＸ、パソコン等の各種データを送信したり、受信したりする端末のことで、暗号化アルゴリズム識別子から暗号化アルゴリズムをディスプレイ等の手段に表示する機能を有し、図１３のような構成になっている。着脱式メモリ読取り装置２３０１は、着脱式メモリ２３０２の動作に必要な電源、クロック、等の制御信号を供給し、データのリード／ライトを行う手段であり、標準インタフェース等を経由して、ＰＨＳ端末本体に接続する手段である。着脱式メモリ２３０２は、メモリ等の素子を高密度実装技術により一体化したもので、メモリ素子の中に今後新たに開発される暗号化アルゴリズムと復号化アルゴリズムと暗号化アルゴリズムを識別する暗号化アルゴリズム識別子を備えていて、マイクロコンピュータの制御プログラムの管理下で着脱式メモリ２３０２の表面に設けられた接点を通して、ＰＨＳ端末本体との情報交換を行う手段である。

【００８６】図３２のように、暗号化装置を備えた既存端末に対して基地局側に本発明の復号化装置を設けることによって、既存端末側で暗号化アルゴリズムを識別するための暗号化アルゴリズム識別子を付加し、基地局側の基地局１の復号化アルゴリズム格納部に格納されている復号化アルゴリズムに対応する暗号化アルゴリズムで暗号化を行えば、既存端末からの情報を受信することができる。逆に基地局側に本発明の暗号化装置を設けることによって、既存端末の復号化アルゴリズムに対応する暗号化アルゴリズムで暗号化を行えば、本発明の基地局側からの情報を既存端末に送信することができる。

【００８７】また、図３３のように、既存基地局に対して、端末側に本発明の暗号化装置を設けることによって、既存基地局の復号化アルゴリズムに対応する暗号化アルゴリズムで暗号化を行えば、本発明の端末側からの情報を既存基地局に送信することができる。逆に既存基地局に対して端末側に本発明の復号化装置を設けることによって、既存基地局で暗号化アルゴリズムを識別するための暗号化アルゴリズムを付加し、端末側のＰＨＳ端末１の復号化アルゴリズム格納部に格納されている復号化アルゴリズムに対応する暗号化アルゴリズムで暗号化を行えば、既存基地局からの情報を受信できる。

【００８８】また、図３４のように、端末側に本発明の暗号化装置を基地局側に本発明の復号化装置を設けることによって、端末側で暗号化アルゴリズムを識別するための識別子を付加するだけで、暗号化アルゴリズム格納部に格納されている暗号化アルゴリズムのいずれかで暗号化を行えば、情報を端末側から基地局側に送信することができる。逆に、端末側に本発明の復号化装置を基地局側に本発明の暗号化装置を設けることによって、基地局側で暗号化アルゴリズムを識別するための識別子を付加するだけで、暗号化アルゴリズム格納部に格納されている暗号化アルゴリズムのいずれかで暗号化を行えば、情報を基地局側から端末側に送信することができる。

【００８９】また、今後新たに開発される暗号化アルゴ

リズムを備えた着脱式メモリを使用した場合も、復号化側で暗号化アルゴリズム識別子をディスプレイ等に表示して、表示したとおりの着脱式メモリを差せば、任意の端末間で情報の伝送を行うことができる。

【００９０】次に図３５に示した本発明における基地局及び管理局について説明する。本発明の無線基地局では、メモリ等からなる記憶部に複数の暗号化／復号化アルゴリズムと、それに対応する識別子、あるいは、ある暗号化から他の暗号化へ直接変換できる暗号化変換アルゴリズムを有している。また、暗号化／復号化アルゴリズム及び暗号化変換アルゴリズムと／に対応する識別子との関係を表すテーブルを記憶するものであってもよい。一方、管理局では複数の無線基地局をその管理下に置いている。

【００９１】ここで、従来の問題点を簡単に説明すると、新しい暗号化アルゴリズムが採用されることになった場合、従来は新しい暗号化アルゴリズムを備えた新しい無線通信端末及び無線基地局等が必要となっていたため、コスト的に大変不利であった。また、インフラの再整備には莫大な費用がかかるため、折角、強力な暗号化アルゴリズムが作られても使用することが困難であった。

【００９２】そこで、この問題を解決する第１の構成として本発明の無線基地局では図９～１２に示したように記憶部が着脱可能（着脱部の構成は図１の無線通信端末と同様に、読取部、装着部、着脱交換記憶装置からなる）であるため容易かつ安価に新しい暗号化／復号化アルゴリズムに対応できる。

【００９３】第２の構成として図３５に示すようには、無線基地局(CS)を管理する管理局のみを新しい暗号化／復号化アルゴリズムに交換しさえすれば、管理局に通信回線で接続された無線基地局の記憶部に反映される構成となっている。

【００９４】ここで無線基地局の記憶部が更新される手順を説明する。まず、管理局の記憶部に新しい暗号化／復号化アルゴリズムを登録する。次に、管理局の支配下に存在する無線基地局に対して、制御部に制御された回線インタフェースは回線接続する。回線接続したのち管理局の制御部は無線基地局に対して、無線基地局の記憶部に記憶されている暗号化／復号化テーブルの更新を命令する命令信号を発する。命令信号を受けた無線基地局では、管理局が通信回線を介して送信してくる暗号化／復号化アルゴリズム及び識別子、暗号化テーブル等を受信し記憶部を更新する。

【００９５】次に図３７から４０に示した本発明の通信システムについて説明する。

【００９６】図３７に示す通信システムは、暗号化／復号化アルゴリズムＡのみを有する無線通信端末(PS1)と暗号化／復号化アルゴリズムＢのみを有する無線通信端末(PS2)とが本発明の無線基地局(CS1)を介すことによって通信する図を示す。本来で有ればPS1とPS2とでは暗号化／復号化アルゴリズムが異なっているため直接通信不可能であるが、無線基地局CS1が複数のアルゴリズムを備え、かつ、呼接続時に発呼者側と着呼者側とが備えている暗号化／復号化アルゴリズムの種類を問い合わせるか、あるいはデータベースから無線通信端末の保有する暗号化／復号化アルゴリズム情報を検索することで、適切な呼接続を行うことができる。このデータベースは位置登録情報などのデータベースを利用すれば安価に構成できよう。

【００９７】また、無線基地局は暗号化／復号化アルゴリズムをＡからＢへ直接変換することができる暗号化変換アルゴリズムを備えてもよい。これを用いれば、高速に変換ができよう。

【００９８】図３８に示した本発明の通信システムでは本発明の無線通信端末と、既存の、あるいは最新の暗号化／復号化アルゴリズムに一部対応できてない無線基地局を介す場合をしめすずである。

【００９９】既存の無線基地局は暗号化に対応していないため暗号化が施されたまま通信データを素通しにする。この場合本発明の無線通信端末では、通信中に相手方の保有する暗号化／復号化アルゴリズムと自局の有するものうち共通のものうちの何れかによって暗号か通信を行うよう設定する。呼接続時あるいは呼接続後に確認された共通の暗号化／復号化アルゴリズムを用いて、図２３のフローチャートに従って暗号化／復号化アルゴリズムを変化させながら通信すればより強力な暗号通信が行えよう。

【０１００】図３９に示した本発明の通信システムでは、複数の無線基地局を介して通信する場合を示している。本発明の無線基地局(CS3, CS4)を介すことにより全ての暗号化／復号化アルゴリズムに対応していない無線通信端末であっても、本発明の無線基地局が全ての暗号化／復号化アルゴリズムに対応しているため何の支障もなく暗号通信が可能となる。

【０１０１】図４０に示した本発明の通信システムでは、無線基地局が全ての暗号化／復号化アルゴリズムに対応できていない場合であっても本発明の無線通信端末を用い、さらに、この無線通信端末間で暗号化／復号化アルゴリズムをハンドシェークすることによって双方の無線区間で暗号化通信が可能となる。

【０１０２】次に本発明の無線通信端末を図４１、４２、４３を用いて説明する。本発明の無線通信端末では、本発明の暗号化／復号化アルゴリズムなどを記憶した着脱交換式のカード型メモリを装着するための装着部４１０２、４２０２、４３０２を備えたものである。これにより、無線通信端末の筐体４１０１、４２０１、４３０１を開くことなく閉じたままで、容易に新たな暗号化／復号化アルゴリズムを記憶したカード型メモリを交換できるものである。これによって、専門の知識を特に

有しないユーザなどであっても、容易に交換できるため、交換サービスをメーカや通信サービス会社が行うことを省略できるため、サービス面でのコストが大幅に削減できる。

【０１０３】また、図４３のようにカード型メモリの装着部に安全のために蓋を設けると良い。これによって装着部から筐体内部へほこりや水滴の進入を防ぐことができるとともに、カード型メモリを保護し、外れて落下することも防止できる。

【０１０４】

【発明の効果】本発明によれば、暗号化アルゴリズムを端末ユーザの暗号化アルゴリズム変更要求時にキー入力等の手段によって任意に又は呼接続時毎に、位置登録時毎に、通話中チャネル切り替え時毎に、認証時時毎に、予め定められた時間毎に、全くランダムな時間毎に、予め定められたエリア毎に、端末が切り替えるという設定を複数行えば、解読されにくい強力な暗号化を行うことができる。又、送信側で暗号化アルゴリズム識別子を付加するだけで、暗号化アルゴリズム格納部１４１１－１～１４１１～Ｎに格納されている暗号化アルゴリズムのいずれかで暗号化を行い、受信側で前記暗号化アルゴリズム識別子を基に復号化アルゴリズム格納部１６１２－１～１６１２～Ｎに格納されている復号化アルゴリズムのいずれかで復号化を行えば、任意の端末間で情報の伝送を行うことができる。又、送信側／受信側で同じ暗号アルゴリズムを備えた着脱式メモリを使用することで、任意の端末間で情報の伝送を行うことができる。つまり、このような暗号化／復号化装置を使うことで、自社、他社を問わずどの端末を使っても音声や様々なデータの通信を行うことができる。

【図面の簡単な説明】

【図１】本発明の無線通信端末を示す図。

【図２】本発明の端末の送信部を示す図。

【図３】本発明の端末の送信部を示す図。

【図４】識別子と暗号化アルゴリズムの対応の例を示す図。

【図５】本発明のＰＨＳ端末送信側のフローチャート図。

【図６】本発明の端末の受信部を示す図。

【図７】本発明の端末の受信部を示す図。

【図８】本発明のＰＨＳ端末受信側のフローチャート図。

【図９】本発明の基地局の送信部を示す図。

【図１０】本発明の基地局の送信部を示す図。

【図１１】本発明の基地局の受信部を示す図。

【図１２】本発明の基地局の受信部を示す図。

【図１３】ＰＨＳの構成図。

【図１４】ＰＨＳ端末機能図。

【図１５】ＰＨＳ端末のブロック図。

【図１６】ＰＨＳ端末送信側のフローチャート図。

【図１７】ＰＨＳ端末受信側のフローチャート図。

【図１８】従来のＰＨＳにおける暗号化部のブロック図。

【図１９】従来のＰＨＳにおける暗号化部のフローチャート図。

【図２０】従来のＰＨＳにおける復号化部のブロック図。

【図２１】従来のＰＨＳにおける復号化部のフローチャート図。

【図２２】本発明の暗号化部のブロック図。

【図２３】本発明の暗号化部のフローチャート図。

【図２４】本発明の復号化部のブロック図。

【図２５】本発明の復号化部のフローチャート図。

【図２６】通信用物理スロットの例を示す図。

【図２７】暗号化アルゴリズム識別子の伝送手順を示す図。

【図２８】暗号化アルゴリズム識別子の受信手順を示す図。

【図２９】着脱式メモリシステムの構成図。

【図３０】本発明の着脱式メモリシステムを利用した暗号化／復号化装置のフローチャート図。

【図３１】本発明の着脱式メモリシステムを利用したＰＨＳ端末を示す図。

【図３２】本発明の暗号化／復号化装置の配置の例を示す図。

【図３３】本発明の暗号化／復号化装置の配置の例を示す図。

【図３４】本発明の暗号化／復号化装置の配置の例を示す図。

【図３５】本発明の管理局と基地局を示す図。

【図３６】本発明の管理局の構成図。

【図３７】本発明の通信システムを示す図。

【図３８】本発明の通信システムを示す図。

【図３９】本発明の通信システムを示す図。

【図４０】本発明の通信システムを示す図。

【図４１】本発明の無線通信端末を示す図。

【図４２】本発明の無線通信端末を示す図。

【図４３】本発明の無線通信端末を示す図。

【符号の説明】

１００･･･マイク、１０１･･･Ａ／Ｄ変換器、１０２･･･音声符号化部、１０３･･･ｄａｔａ ｓｅｌｅｃｔｏｒ部、１０４･･･暗号化部、１０５･･･ｄａｔａ ｂｌｏｃｋ生成部、１０６･･･誤り検出訂正符号化部、１０７･･･変調部、１０８･･･無線部、１０９･･･外部インタフェース部、１１０･･･暗号ｓｅｌｅｃｔｏｒ部、１１１･･･キー入力部、１１２･･･制御部、１１３･･･記憶部、１１４･･･読取部、１１５･･･着脱式記憶部、１１６･･･装着部、１２０･･･スピーカ、１２１･･･Ｄ／Ａ変換器、１２２･･･音声復号化部、１２３･･･ｄａｔａ判定部、１２４･･･復号化部、１２５･･･ｄａｔａ分割部、１２６･･･誤

37

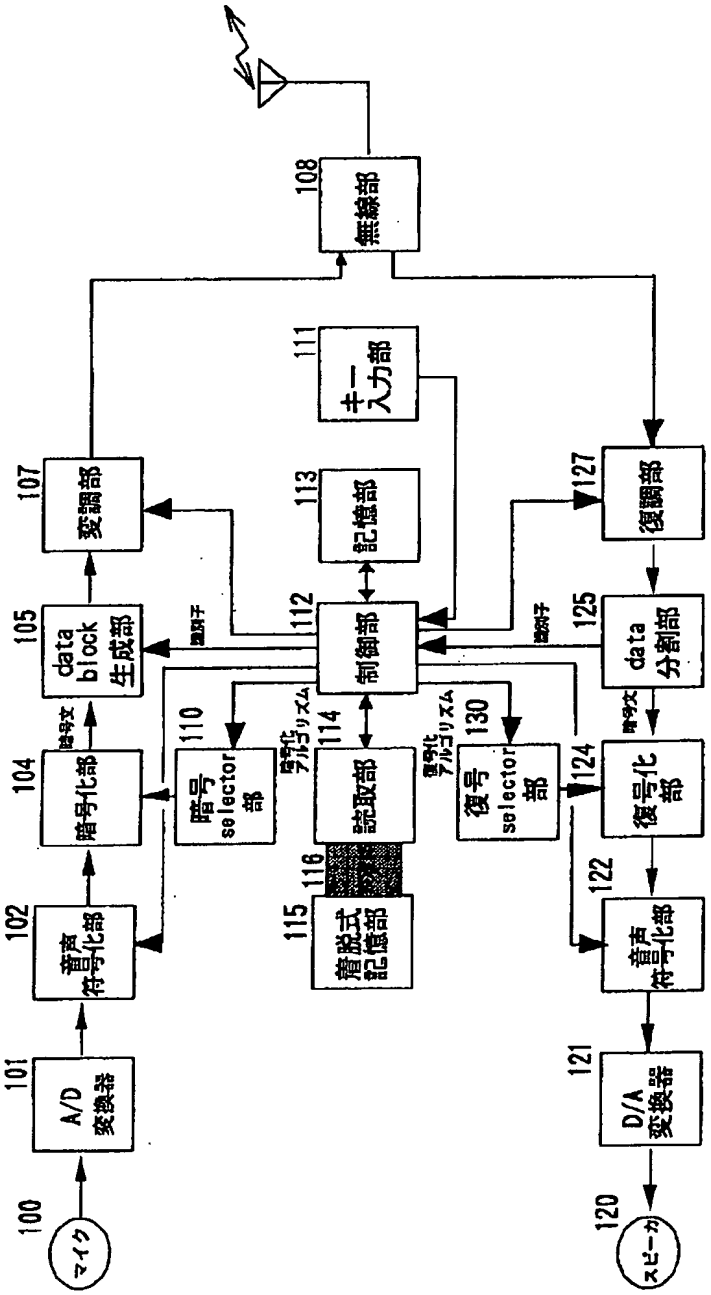
り検出訂正部、１２７･･･復調部、１２８･･･無線部、１２９･･･外部インタフェース部、１３０･･･復号ｓｅｌｅｃｔｏｒ部、１３１･･･キー入力部、１３２･･･制御部、１３３･･･記憶部、１４０･･･ＰＢＸ、１４１･･･ＤＳＵ、１４２･･･ＳＩＮＦ、１４３･･･エコーキャンセラ、１４４･･･音声符号化部、１４５･･･暗号化部、１４６･･･ｄａｔａ ｂｌｏｃｋ生成部、１４７･･･誤り検出訂正符号化部、１４８･･･変調部、１４９･･･無線部、１５０＊

38

＊･･･暗号ｓｅｌｅｃｔｏｒ部、１５１･･･制御部、１５２･･･記憶部、１６０･･･ＰＢＸ、１６１･･･ＤＳＵ、１６２･･･ＳＩＮＦ、１６３･･･エコーキャンセラ、１６４･･･音声復号化部、１６５･･･復号化部、１６６･･･ｄａｔａ分割部、１６７･･･誤り検出訂正部、１６８･･･復調部、１６９･･･無線部、１７０･･･復号ｓｅｌｅｃｔｏｒ部、１７１･･･制御部、１７２･･･記憶部

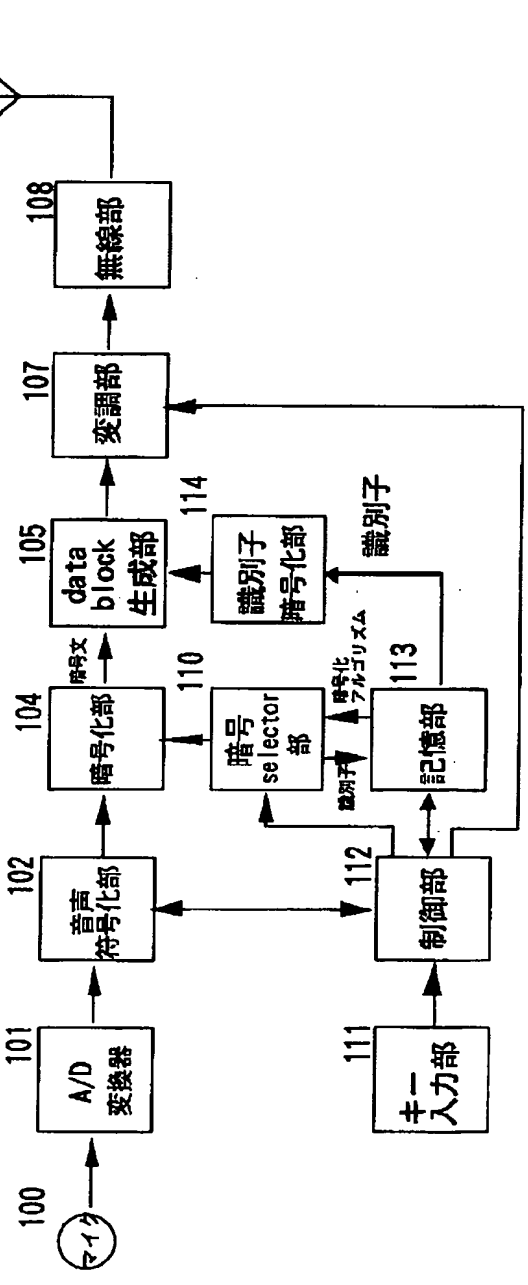
【図１】

図 1



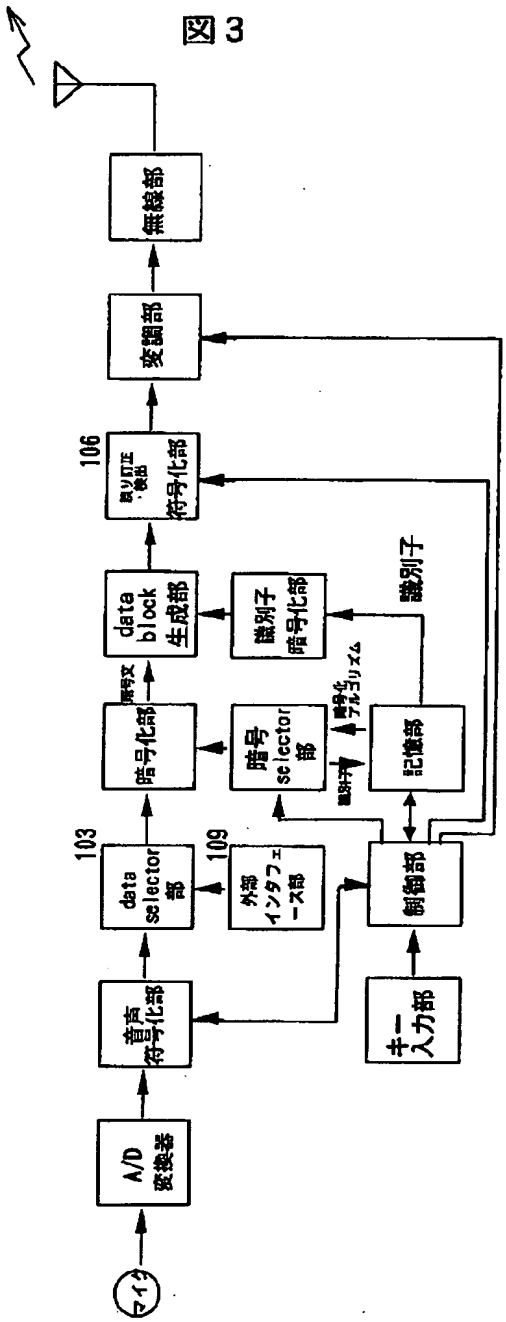
【図２】

図 2



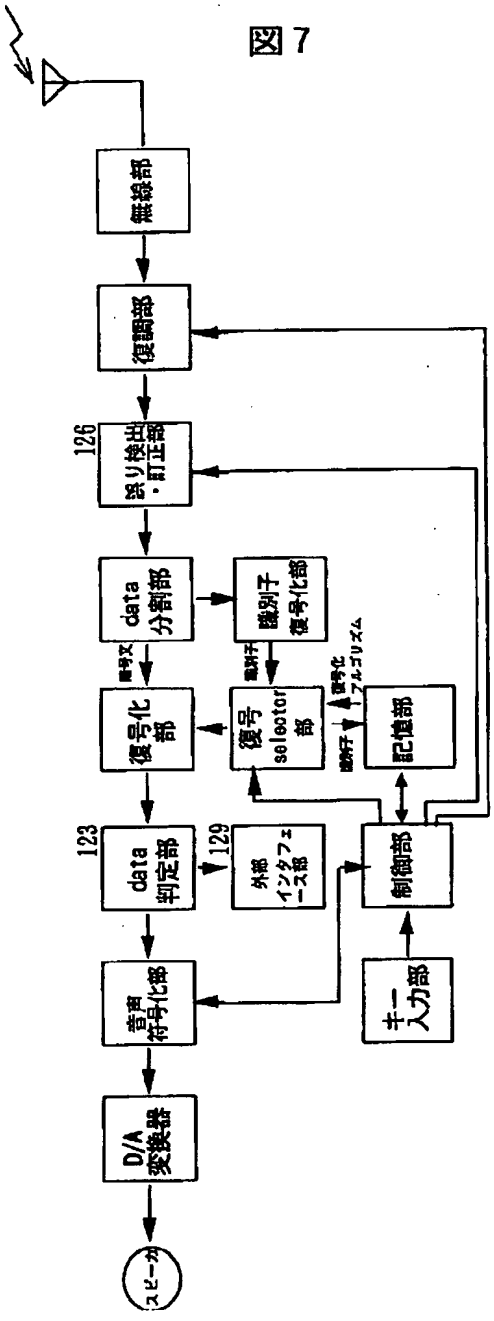
【図３】

図３


無線部
変調部
106
誤り訂正符号化部
data block 生成部
識別子暗号化部
暗号化
暗号文
暗号化アルゴリズム
暗号 selector 部
記憶部
識別子
103
data selector 部
109
外部インタフェース部
制御部
音声符号化部
キー入力部
A/D 変換器
マイク

【図７】

図７


無線部
復調部
126
誤り検出・訂正部
data 分割部
識別子復号化部
復号化
暗号文
復号化アルゴリズム
復号 selector 部
記憶部
123
data 判定部
129
外部インタフェース部
制御部
音声符号化部
キー入力部
D/A 変換器
スピーカ

【図４】

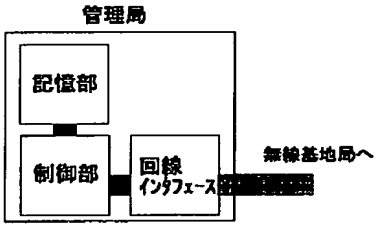
図 4

識別子	暗号化アルゴリズム	復号化アルゴリズム
000	D	D^{-1}
001	F	F^{-1}
002	M	M^{-1}
・	・	・
・	・	・
・	・	・

注）復号化アルゴリズムの－１は暗号化アルゴリズムの逆関数であることを示す。

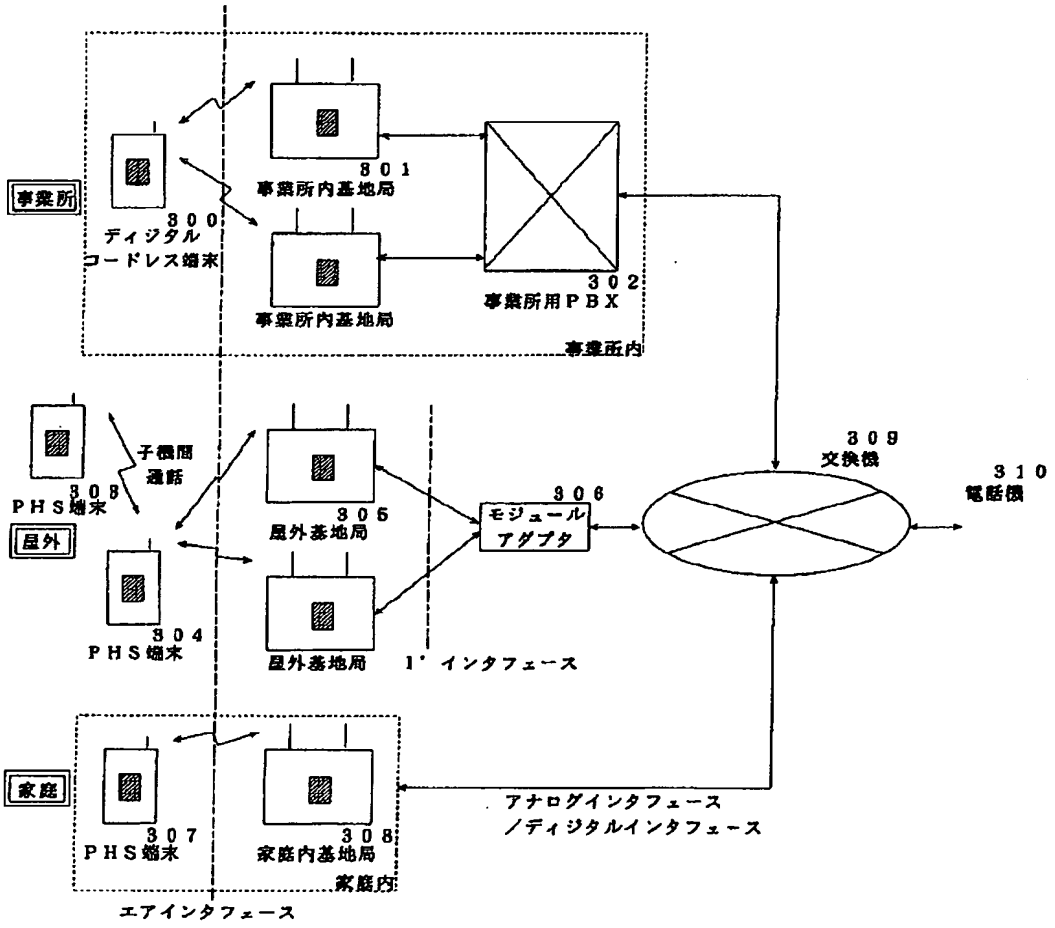
【図３６】

図36



【図１３】

図 13

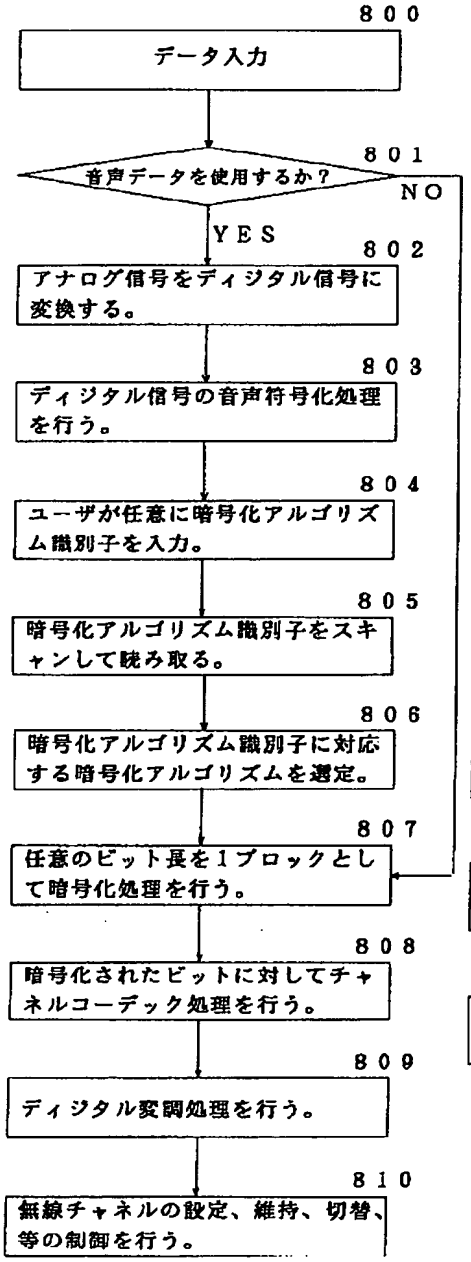


▨暗号化／復号化部

I' インタフェース：［基本アクセスインタフェース（２Ｂ＋Ｄ）］×２

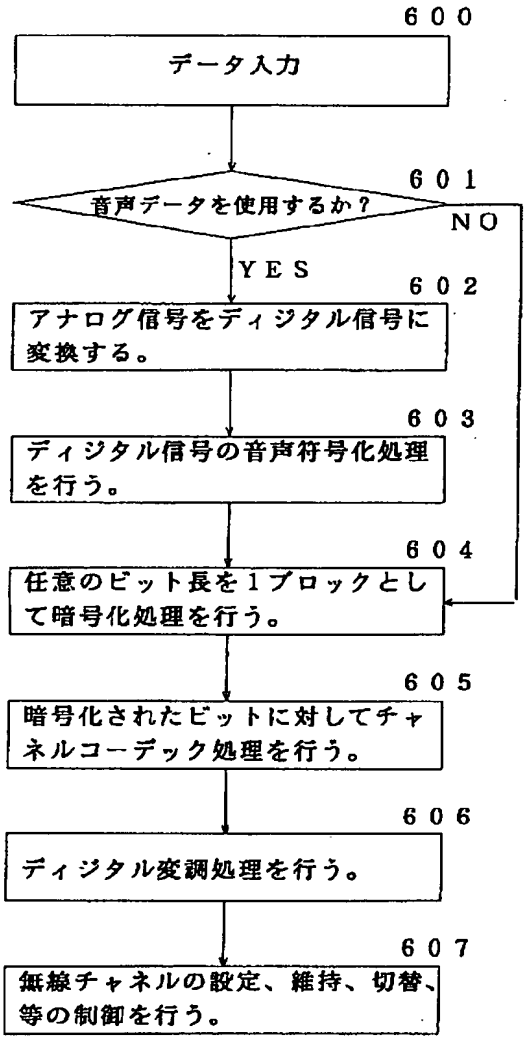
【図５】

図 5



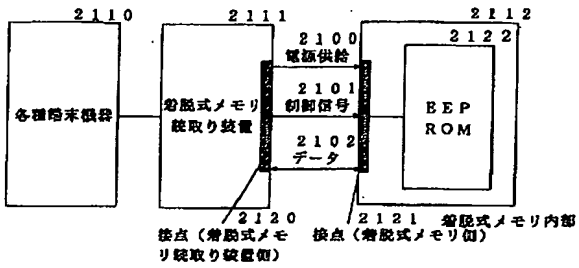
【図１６】

図 16



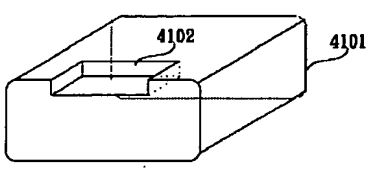
【図２９】

図 29



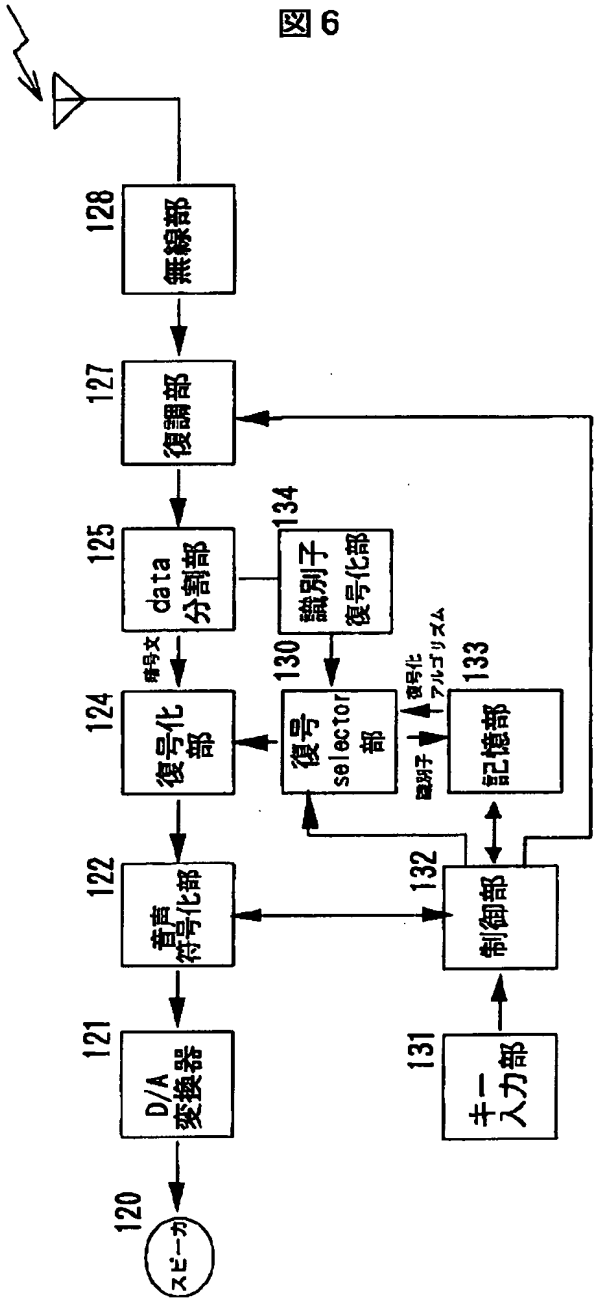
【図４１】

図41



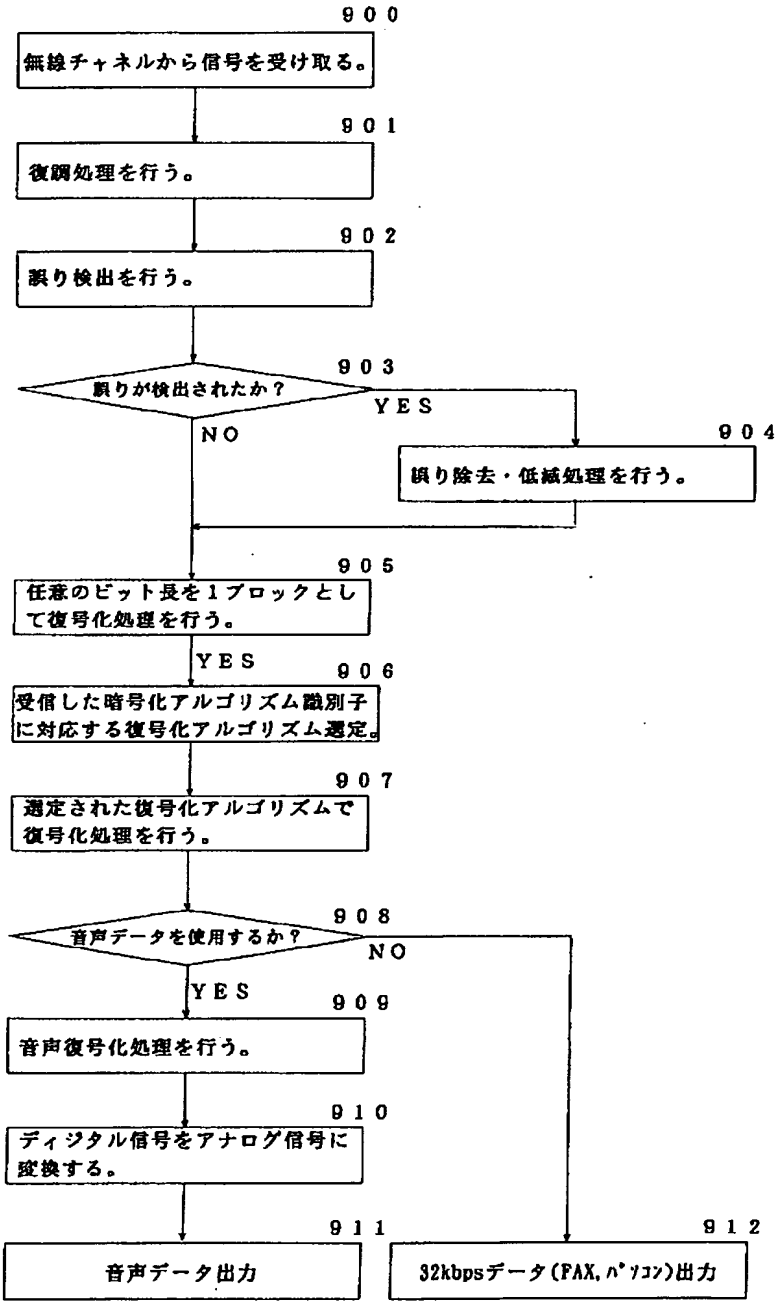
【図６】

図６


128
無線部
127
復調部
125
data
分割部
134
識別子
復号化部
暗号文
130
復号
selector
部
復号化
アルゴリズム
133
記憶部
識別子
124
復号化
部
122
音声
符号化部
132
制御部
121
D/A
変換器
131
キー
入力部
120
スピーカ

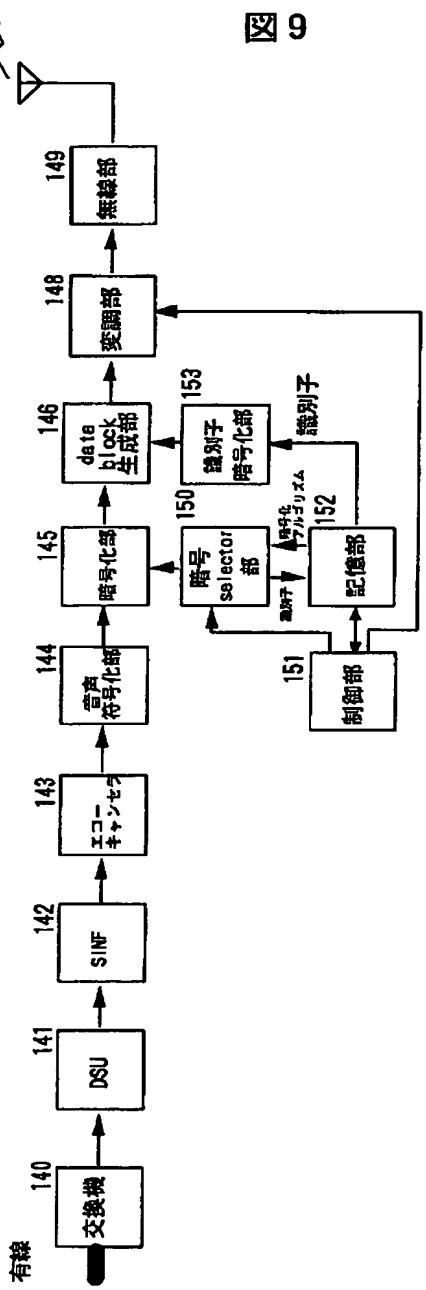
【図８】

図 8


９００
無線チャネルから信号を受け取る。
９０１
復調処理を行う。
９０２
誤り検出を行う。
９０３
誤りが検出されたか？
YES
NO
９０４
誤り除去・低減処理を行う。
９０５
任意のビット長を１ブロックとして復号化処理を行う。
YES
９０６
受信した暗号化アルゴリズム識別子に対応する復号化アルゴリズム選定。
９０７
選定された復号化アルゴリズムで復号化処理を行う。
９０８
音声データを使用するか？
NO
YES
９０９
音声復号化処理を行う。
９１０
ディジタル信号をアナログ信号に変換する。
９１１
音声データ出力
９１２
32kbpsデータ(FAX, ﾊﾟｿｺﾝ)出力

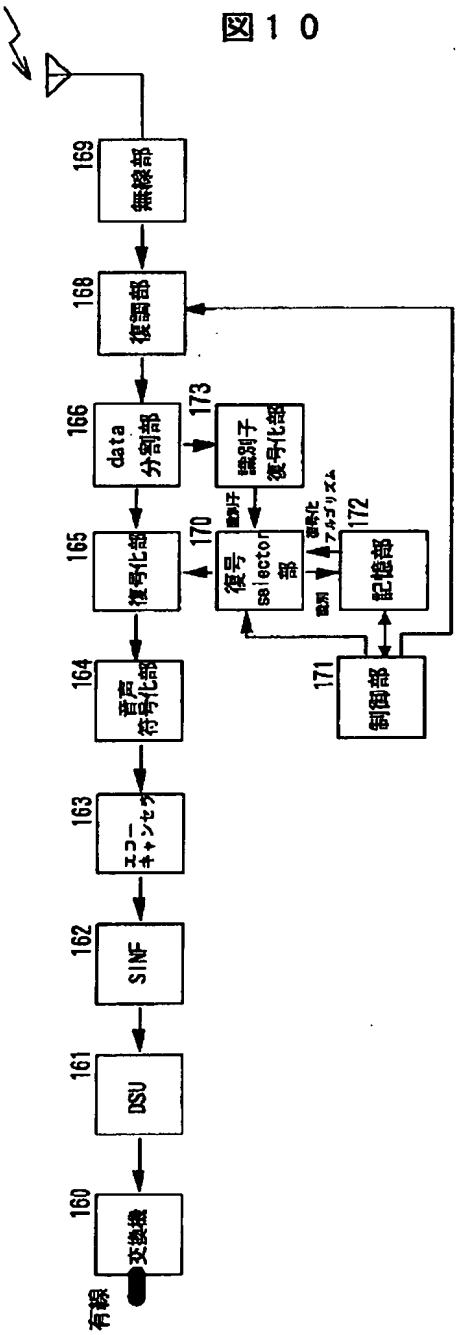
【図９】

図９


有線
140
交換機
141
DSU
142
SINF
143
エコーキャンセラ
144
音声符号化部
145
暗号化部
146
data block 生成部
148
変調部
149
無線部
150
暗号 selector 部
151
制御部
152
記憶部
153
識別子暗号化部
識別子
暗号化アルゴリズム

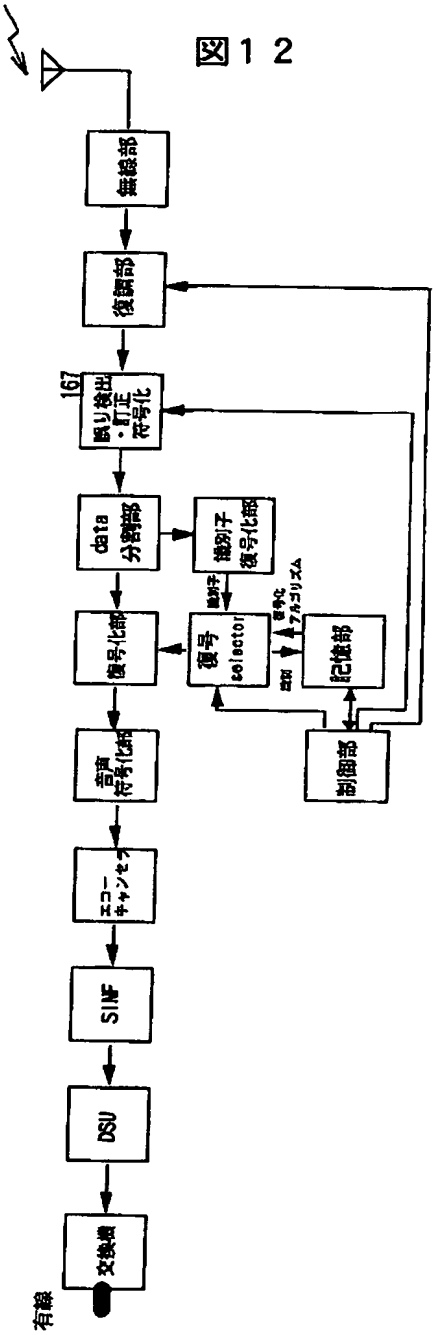
【図１０】

図１０



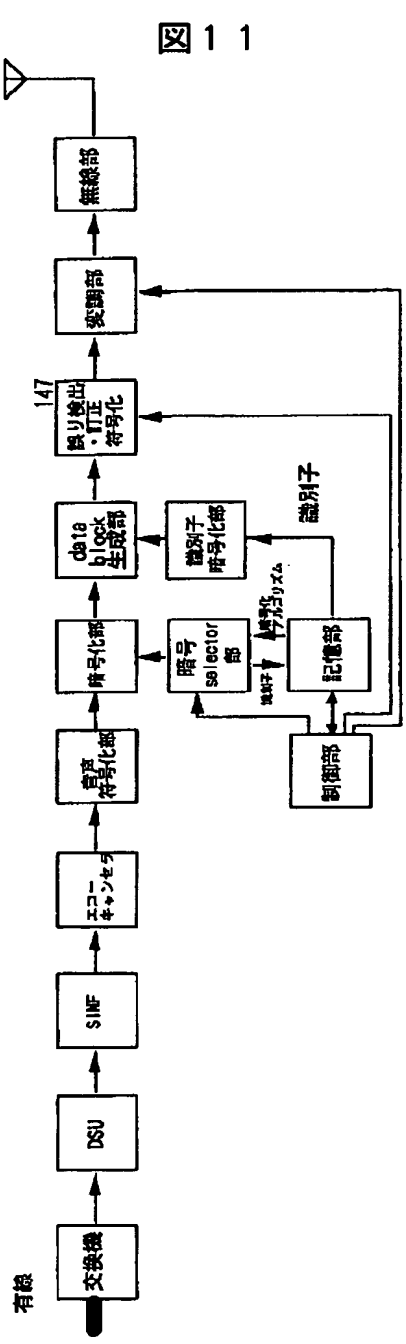
【図１２】

図１２



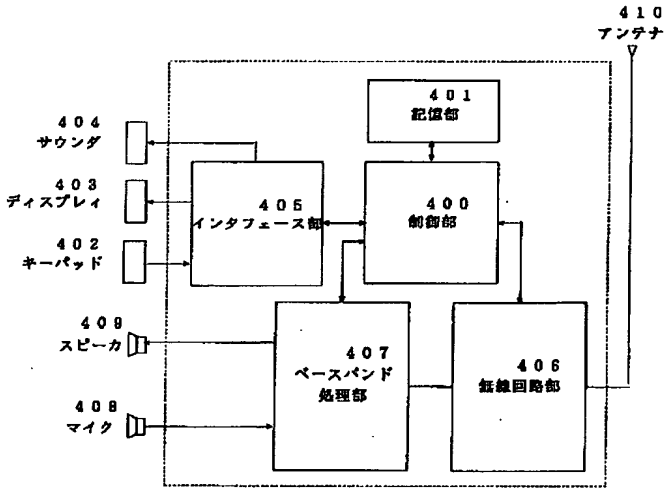
【図１１】

図１１


有線
交換機
DSU
SIMF
エコーキャンセラ
音声符号化部
符号化部
暗号 selector 部
data block 生成部
識別子符号化部
147
誤り検出・訂正符号化
変調部
無線部
記憶部
制御部
識別子
暗号アルゴリズム

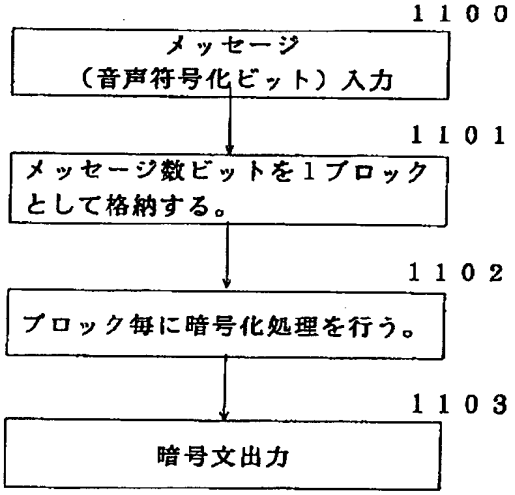
【図１４】

図 14



【図１９】

図 19



【図１５】

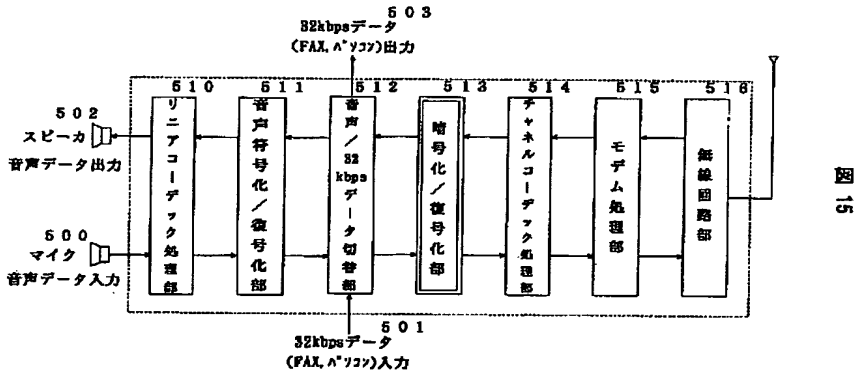
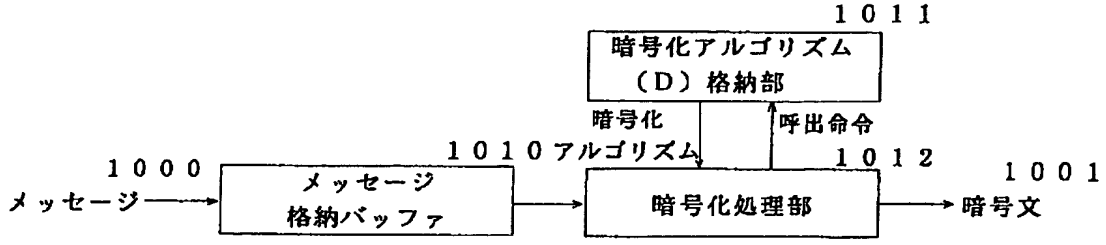


図 15

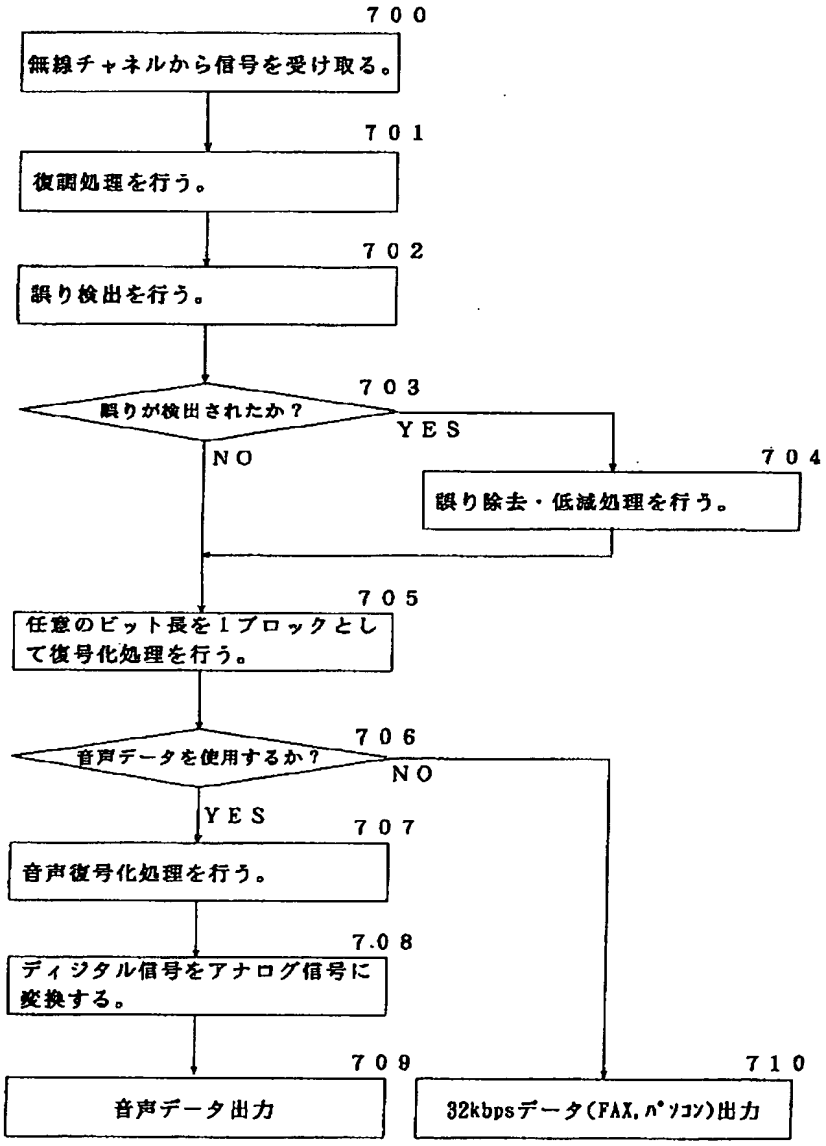
【図１８】

図 18



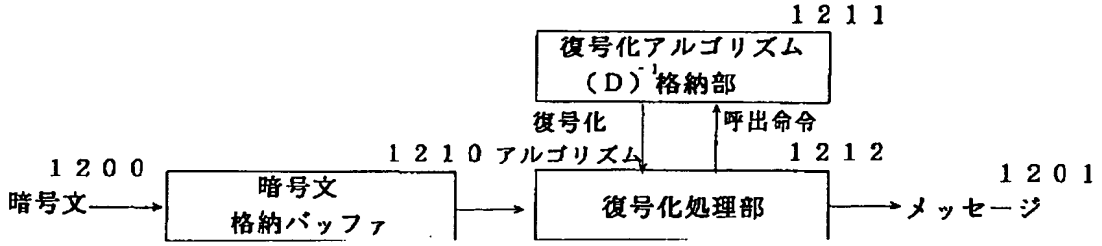
【図１７】

図 17


７００
無線チャネルから信号を受け取る。
７０１
復調処理を行う。
７０２
誤り検出を行う。
７０３
誤りが検出されたか？
ＹＥＳ
ＮＯ
７０４
誤り除去・低減処理を行う。
７０５
任意のビット長を１ブロックとして復号化処理を行う。
７０６
音声データを使用するか？
ＮＯ
ＹＥＳ
７０７
音声復号化処理を行う。
７０８
ディジタル信号をアナログ信号に変換する。
７０９
音声データ出力
７１０
32kbpsデータ(FAX,ﾊﾟｿｺﾝ)出力

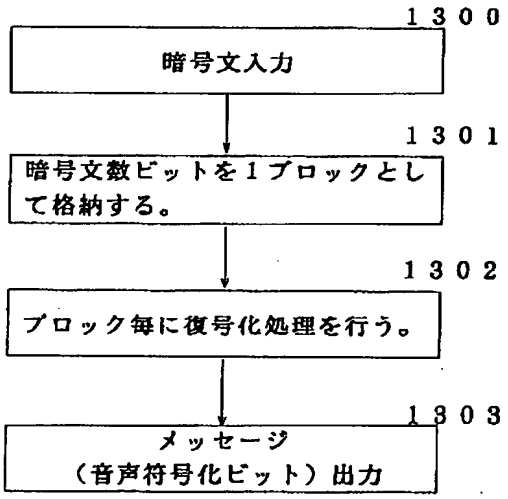
【図２０】

図 20



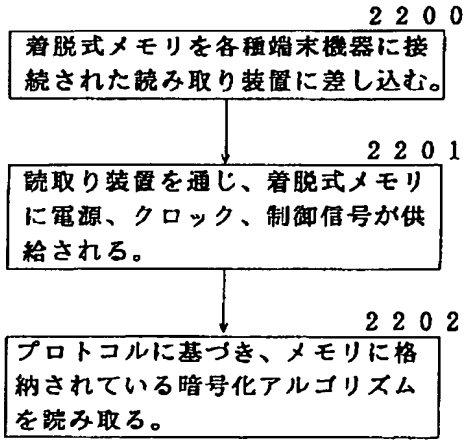
【図２１】

図 21



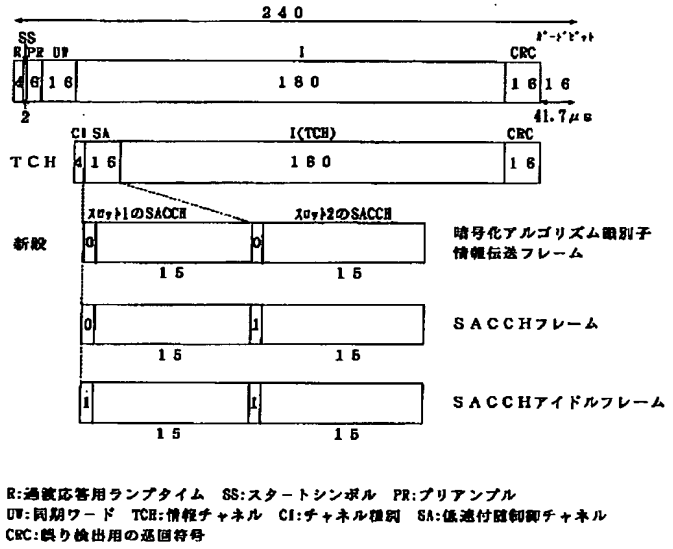
【図３０】

図 30



【図２６】

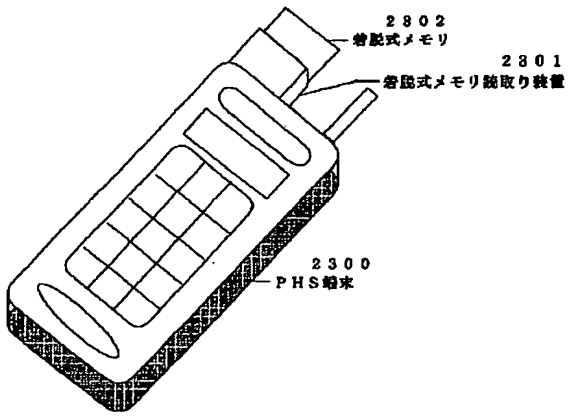
図 26



R:通話応答用ランプタイム　SS:スタートシンボル　PR:プリアンブル
UW:同期ワード　TCH:情報チャネル　CI:チャネル種別　SA:低速付随制御チャネル
CRC:誤り検出用の巡回符号

【図３１】

図 31



【図２２】

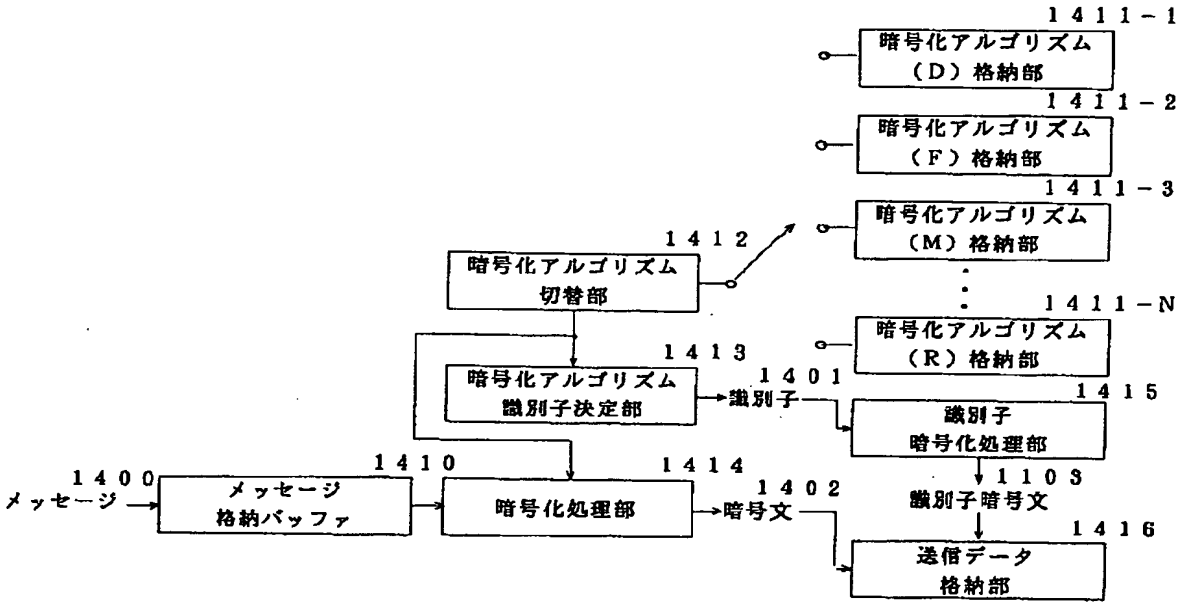
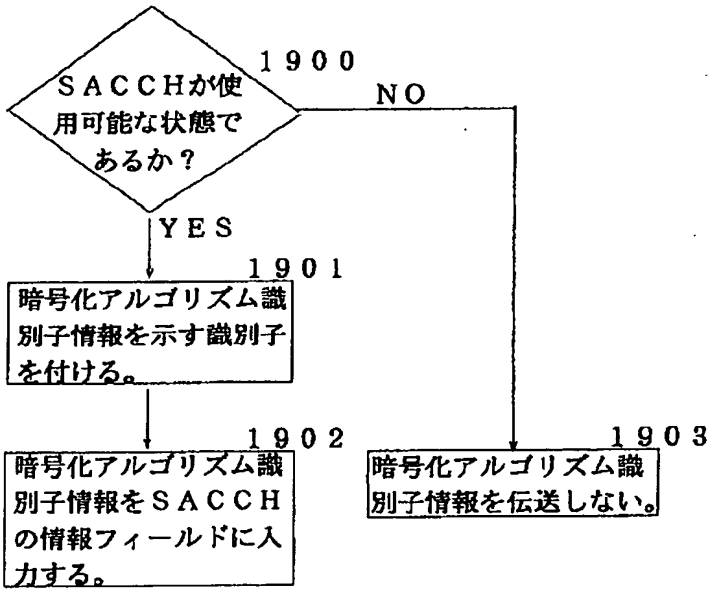


図22

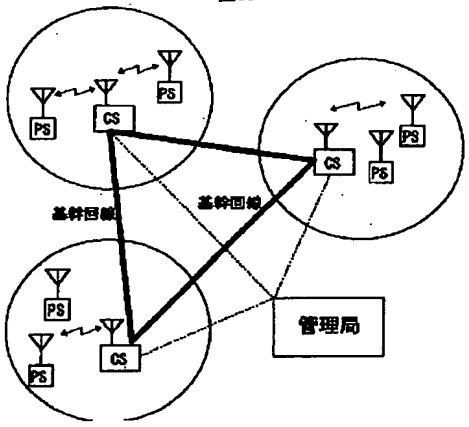
【図２７】

図 27



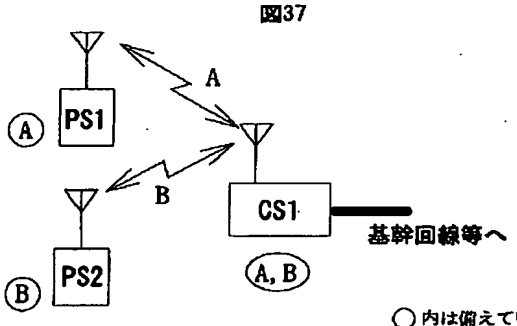
【図３５】

図35



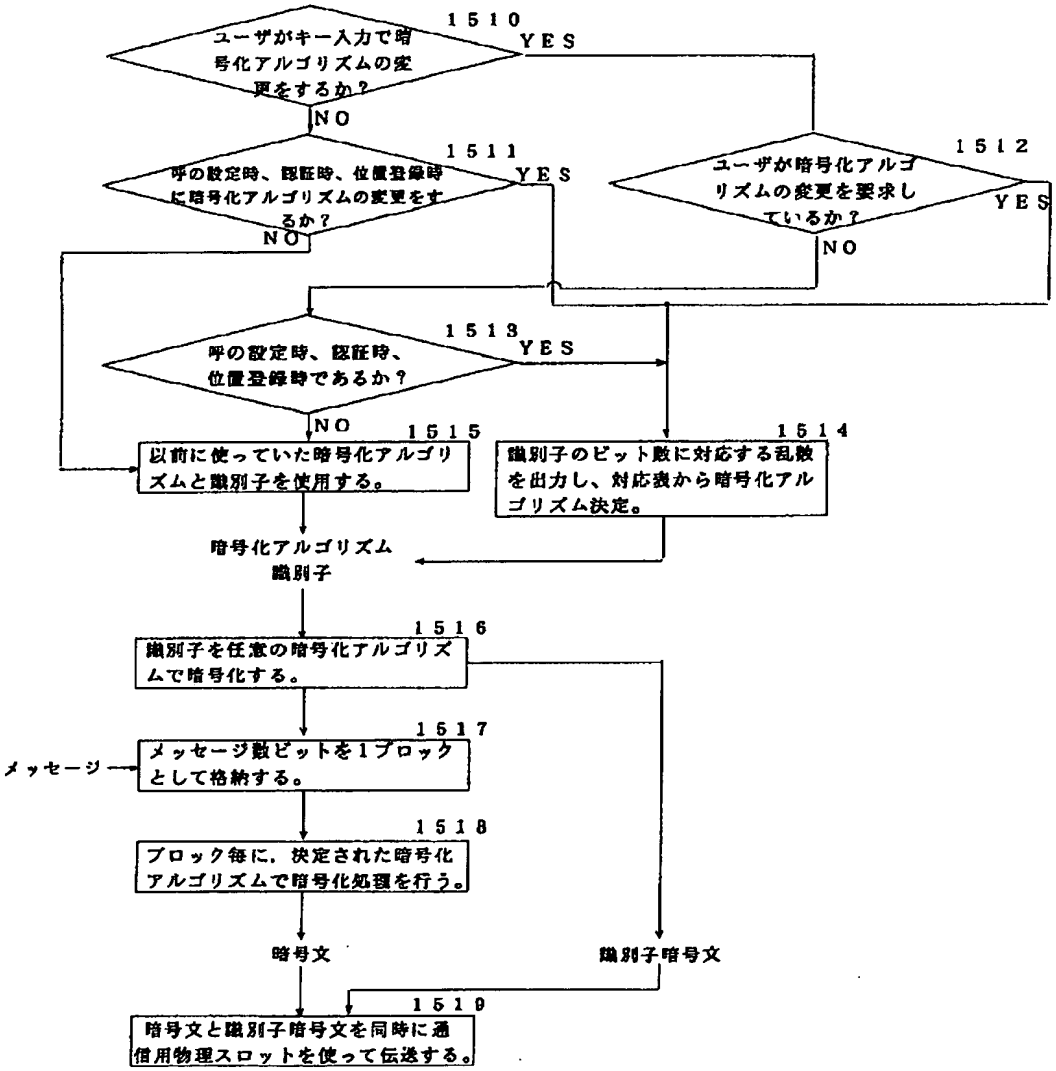
【図３７】

図37

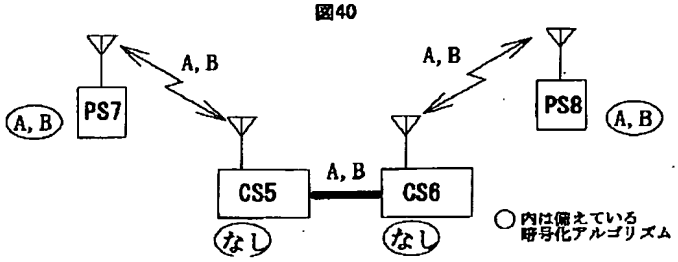


【図２３】

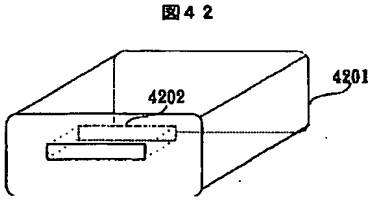
図 23



【図４０】

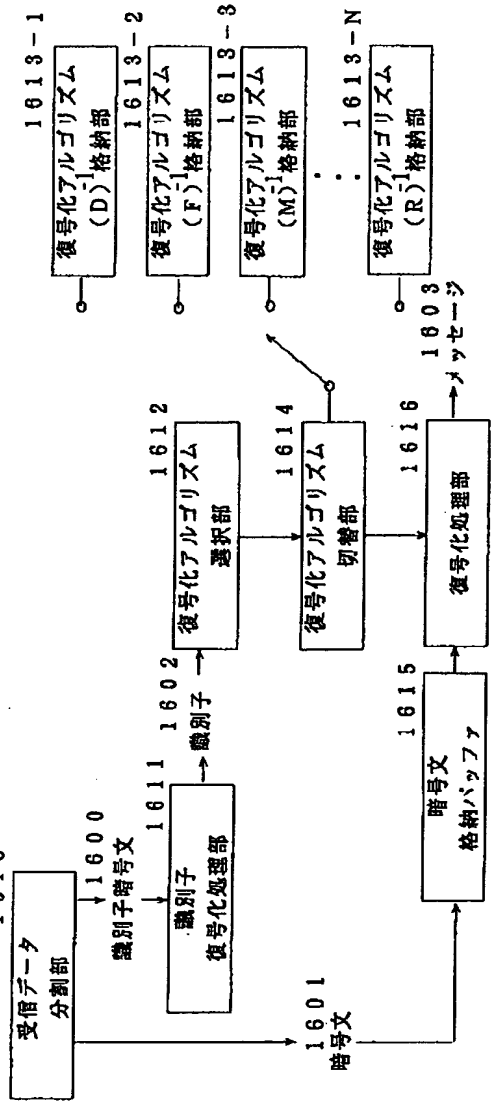


【図４２】



【図２４】

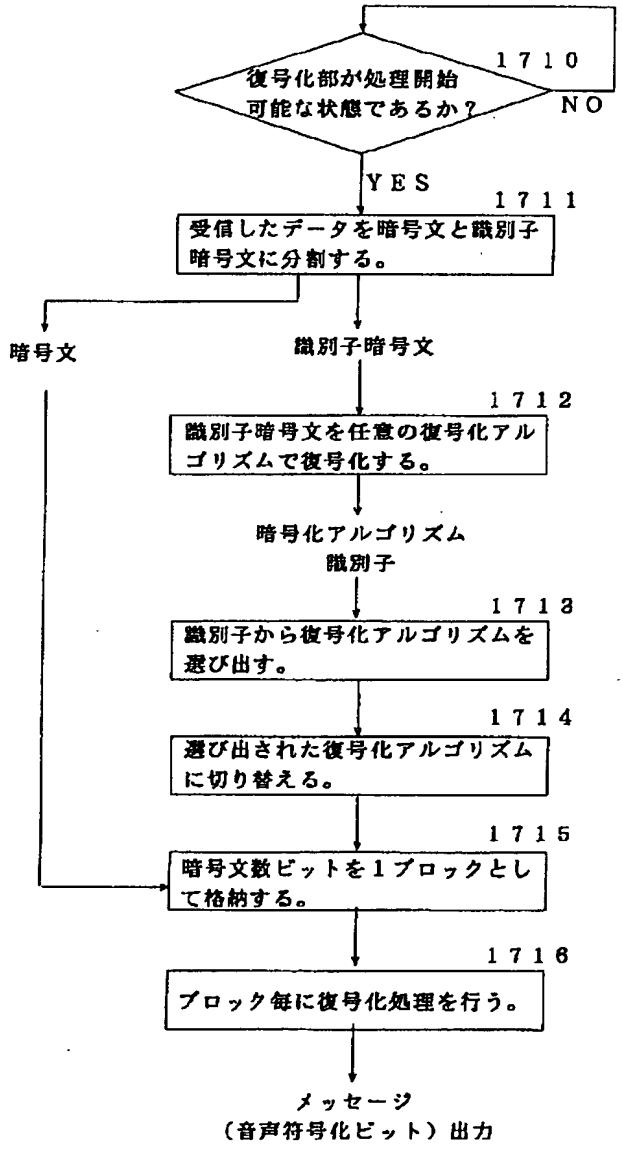
図 24



注）図中の復号化アルゴリズム格納部の中の
－１は暗号化アルゴリズムの逆関数を示す。

【図２５】

図 25


1710
復号化部が処理開始可能な状態であるか？
NO
YES
1711
受信したデータを暗号文と識別子暗号文に分割する。
暗号文
識別子暗号文
1712
識別子暗号文を任意の復号化アルゴリズムで復号化する。
暗号化アルゴリズム識別子
1713
識別子から復号化アルゴリズムを選び出す。
1714
選び出された復号化アルゴリズムに切り替える。
1715
暗号文数ビットを１ブロックとして格納する。
1716
ブロック毎に復号化処理を行う。
メッセージ（音声符号化ビット）出力

【図４３】

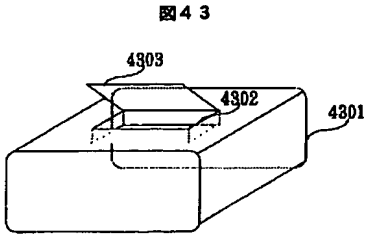
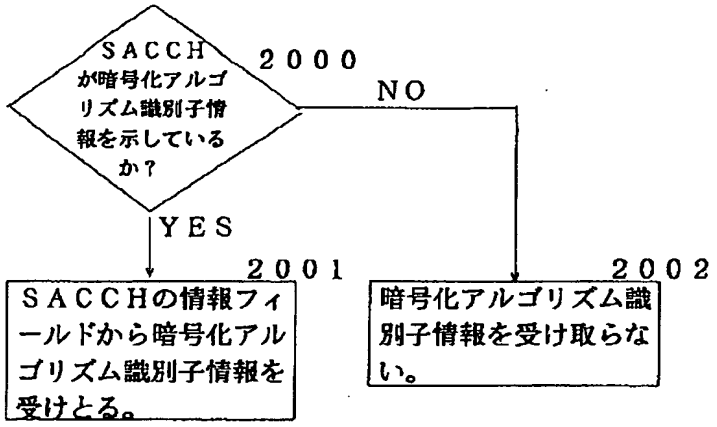


図43
4303
4302
4301

【図２８】

図 28



【図３４】

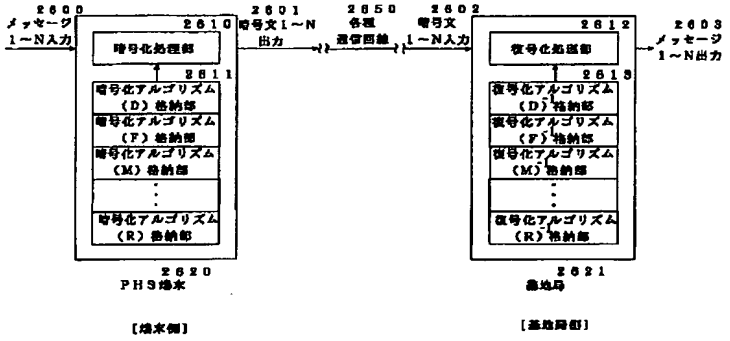
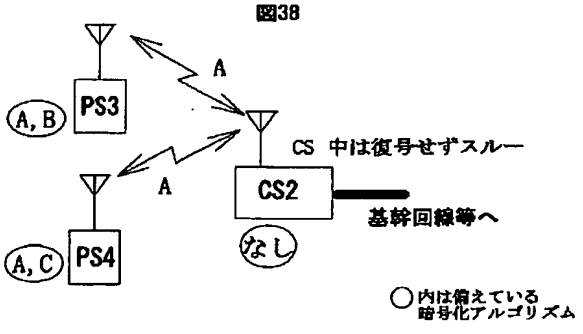
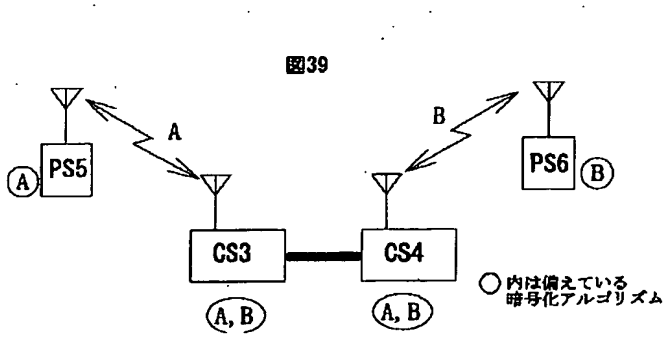


図 34

【図３８】

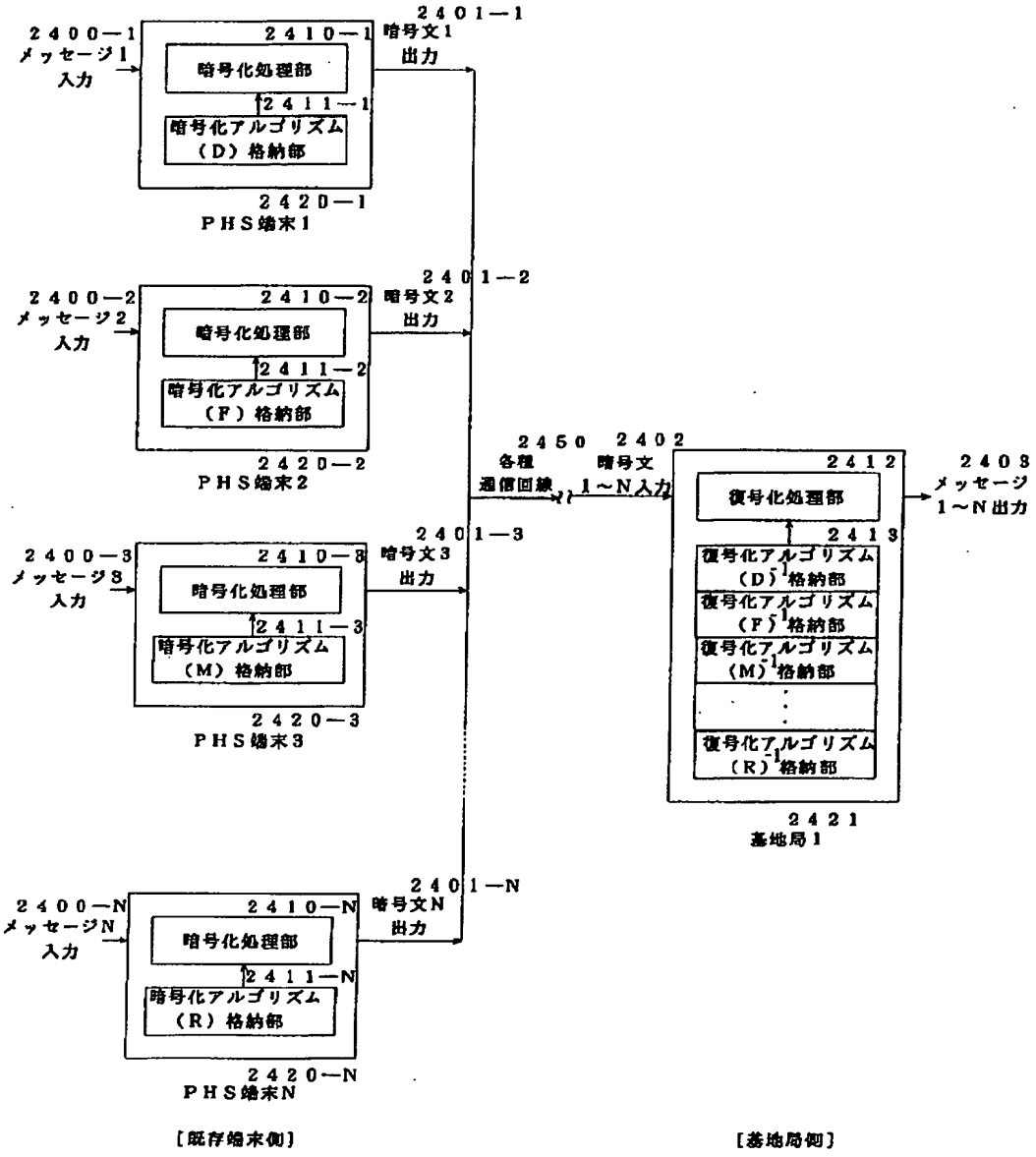


【図３９】



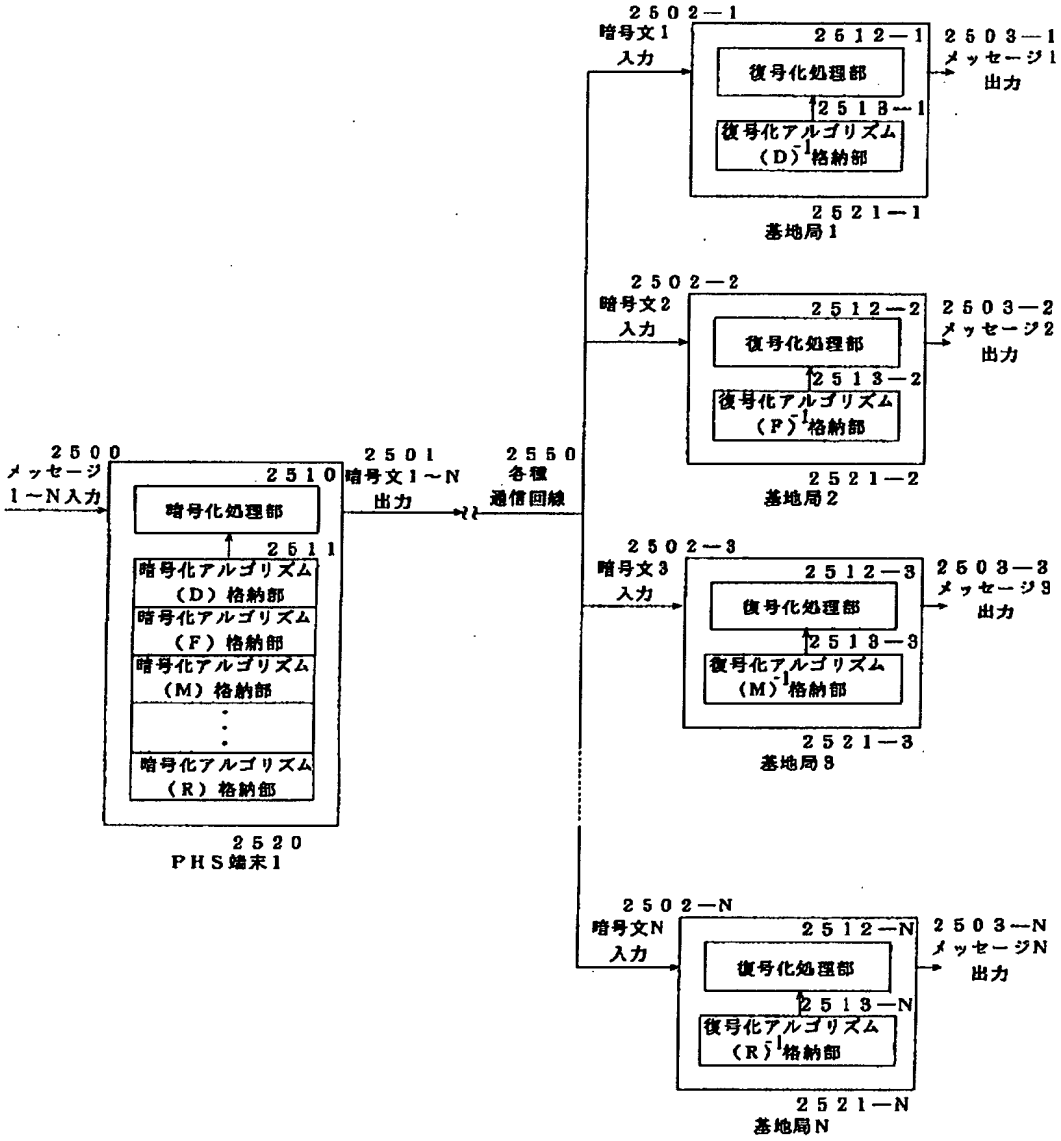
【図３２】

図 32


2400－1
メッセージ1
入力
2410－1
暗号化処理部
2411－1
暗号化アルゴリズム
（D）格納部
2420－1
PHS端末1
2401－1
暗号文1
出力
2400－2
メッセージ2
入力
2410－2
暗号化処理部
2411－2
暗号化アルゴリズム
（F）格納部
2420－2
PHS端末2
2401－2
暗号文2
出力
2400－3
メッセージ3
入力
2410－3
暗号化処理部
2411－3
暗号化アルゴリズム
（M）格納部
2420－3
PHS端末3
2401－3
暗号文3
出力
2400－N
メッセージN
入力
2410－N
暗号化処理部
2411－N
暗号化アルゴリズム
（R）格納部
2420－N
PHS端末N
2401－N
暗号文N
出力
2450
各種
通信回線
2402
暗号文
1～N入力
2412
復号化処理部
2413
復号化アルゴリズム
（D）$^{-1}$格納部
復号化アルゴリズム
（F）$^{-1}$格納部
復号化アルゴリズム
（M）$^{-1}$格納部
復号化アルゴリズム
（R）$^{-1}$格納部
2421
基地局1
2403
メッセージ
1～N出力
［既存端末側］
［基地局側］

【図３３】

図 33


２５００
メッセージ
１～N入力
２５１０
暗号化処理部
２５１１
暗号化アルゴリズム
（D）格納部
暗号化アルゴリズム
（F）格納部
暗号化アルゴリズム
（M）格納部
暗号化アルゴリズム
（R）格納部
２５２０
PHS端末1
２５０１
暗号文1～N
出力
２５５０
各種
通信回線
２５０２－１
暗号文1
入力
２５１２－１
復号化処理部
２５１３－１
復号化アルゴリズム
（D）-1格納部
２５２１－１
基地局1
２５０３－１
メッセージ1
出力
２５０２－２
暗号文2
入力
２５１２－２
復号化処理部
２５１３－２
復号化アルゴリズム
（F）-1格納部
２５２１－２
基地局2
２５０３－２
メッセージ2
出力
２５０２－３
暗号文3
入力
２５１２－３
復号化処理部
２５１３－３
復号化アルゴリズム
（M）-1格納部
２５２１－３
基地局3
２５０３－３
メッセージ3
出力
２５０２－N
暗号文N
入力
２５１２－N
復号化処理部
２５１３－N
復号化アルゴリズム
（R）-1格納部
２５２１－N
基地局N
２５０３－N
メッセージN
出力
［端末側］
［既存基地局側］